Heron Park Primary Academy

SPHPPA10

Online Safety including Social Media Policy

Autumn 2017- Autumn 2018

East Sussex County Council believes that the safe use of information and communication technologies in schools and education settings brings great benefits. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This policy template will help schools and settings to form an online safety (or 'e-Safety') policy that is appropriate to their needs and requirements.

This policy template and guidance has also been produced as part of ongoing work on the East Sussex Local Safeguarding Children Board (LSCB) priority to coordinate a multi-agency approach to online safety for children, young people and families. The LSCB action plan for online safety includes: improving professionals' knowledge about e-safety and support to children, young people and parents keep safe online.

This policy template and guidance has been commissioned by the East Sussex Standards and Learning Effectiveness Service (SLES) and is based on the work of the Kent County Council and the Kent Safeguarding Children's Board Online Safety (e-Safety) Strategy Group. Contributions have also been made by the East Sussex LSCB, and by East Sussex's Schools ICT Team.

Online Safety (e–Safety) Policy and Guidance for Education Settings 2016

Contents

1. Creating an Online Safety Ethos

1.1. Aims and policy scope

Relevant for all settings

Guidance: Why does a school/setting need an online safety or "e-Safety" policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety or online safety covers issues relating to children and young people as well as adults, and their safe use of the Internet, mobile phones, tablets and other electronic communications technologies, both in and out of school or settings. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. It should be noted that the use of the term 'online safety' rather than "e-Safety" reflects a widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues and a move away from a focus as online safety as an ICT issue.

Online safety is an essential element of all education settings safeguarding responsibilities and requires strategic oversight and ownership to be able to develop appropriate policies and procedures to protect and prepare all members of the community. The online safety agenda has shifted towards enabling children and young people to manage risk and requires a comprehensive and embedded curriculum which is adapted specifically to the needs and requirements of children and the setting. Online safety should be embedded throughout settings safeguarding practice and is clearly identified as an issue for leaders and managers to consider and address.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Schools and settings must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good online safety practice in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an online safety policy can and have led to civil, disciplinary and criminal action being taken against staff, children and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have and a clearly embedded and understood policy can enable education leaders and managers to ensure that safe practice is established. The online safety policy is essential in setting out how the school plans to develop and establish its approach and to identify core principles which all members of the community need to be aware of and understand.

Leaders and managers within education settings will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities as well as promoting personal enjoyment and achievements for all members of the community. It is essential that the use of ICT and online tools is carefully managed by educational settings to ensure that all members of the community are kept safe and that online risks and dangers are recognised by the setting and mitigated.

Children and young people are likely to encounter a range of risks online highlighted as content, contact and conduct (also identified within Annex C of 'Keeping Children Safe in Education' 2016). These issues can be summarised as:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as recipient	Advertising Spam Copyright Sponsorship	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading information/advice Body image and self esteem Distressing or offensive content
Contact Child as participant	Tracking Harvesting Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including “sexting”) Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or “Addiction” Plagiarism

Content adapted from EU Kids Online 2008

‘Keeping Children Safe in Education (KCSiE)’ is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Non-Maintained Special Schools (England) Regulations 2015. It applies to all schools and colleges, whether maintained, non-maintained or independent, including academies and free schools, alternative provision academies, maintained nursery schools, pupil referral units and all further education colleges and sixth-form colleges and relates to responsibilities towards children under the age of 18.

All schools and colleges must have regards to KCSiE when carrying out their duties to safeguard and promote the welfare of children and schools and colleges should comply with the guidance unless exceptional circumstances arise. KCSiE 2016 highlights online safety as a safeguarding issue for schools and colleges and therefore it must be considered and implemented within schools and settings statutory safeguarding responsibilities.

KCSiE 2016 highlights a range of specific statutory responsibilities for schools and colleges regarding online safety which governing bodies and proprietors need to be aware of. This includes (but is not limited to)the need for all staff to be aware of the role of technology within sexual and emotional abuse and also Child Sexual Exploitation and radicalisation and the need for all staff to be aware that abuse can be perpetrated by children themselves and specifically identifies sexting and cyberbullying.

Education settings will need to be mindful of the role of Ofsted and the practice expectations regarding online safety within the Common Inspection Framework (CIF) , Inspecting Safeguarding briefing and supporting documents (August 2016 and subsequent updates) which highlights online safety as part of safeguarding for maintained schools and academies, non-association independent schools, further education and skills provision and early years settings as part of role and responsibilities under "Effectiveness of leadership and management" and "Personal development, behaviour and welfare".

The online safety (e-Safety) policy will need to be interlinked with many different school/setting policies including the Child Protection and Safeguarding Policy, Anti-Bullying, Home School agreement, Behaviour and School Development Plan and should relate to other policies including those for personal, social and health education (PSHE) and for citizenship.

Online Safety policies will provide education settings with an essential framework to develop their online safety ethos as part of safeguarding and enable leaders and managers to set out strategic approaches and considerations as well as ways to monitor impact. It is essential that the online safety policies are implemented as part of the settings safeguarding roles and responsibilities

1.1. Statements:

- Heron Park Primary Academy believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- *Heron Park Primary Academy* identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- *Heron Park Primary Academy* has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions.
- *Heron Park Primary Academy* identifies that there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of *Heron Park Primary Academy* online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that *Heron Park Primary Academy* is a safe and secure environment.
    - Safeguard and protect all members of *Heron Park Primary Academy* community online.
    - Raise awareness with all members of *Heron Park Primary Academy* community regarding the potential risks as well as benefits of technology.
    - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

1.2 Writing and reviewing the online safety policy

Relevant for all settings

Guidance:

Education leaders and managers including Governing Bodies or other strategic bodies such as trusts, boards or committees, must be involved in creating and reviewing the online safety policy, at least annually and must also take an active role in monitoring its impact. Leaders and managers will need to ensure that they take responsibility for revising the online safety policy and practice where necessary (such as after an incident or change in national or local guidance or legislation). The headteacher, manager and Governing body have a legal responsibility to safeguard children and staff and this will include online activity.

It is strongly recommended that schools and settings work with stakeholders when constructing and reviewing the policy to ensure that a sense of ownership is developed. The more that staff, parents, governors and pupils are involved in deciding and creating the policy, then the more effective it will be in the long term.

1.2 Statements:

The Designated Safeguarding Leads (DSL) are: Mrs Anne Wilson & Mrs Debra Robinson

The School Online safety (e-Safety) lead for the Governing Body is: Mrs Trudy Hillman

Policy approved by Head Teacher: Mr Raja Ali Date: September 2017

Policy approved by Governing Body (LAB): Mrs Karen Rolf (Chair of LAB) Date: September 2107

The date for the next policy review is: September 2018

- Heron Park Primary Academy online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the East Sussex County Council (ESCC) online safety policy template, with specialist advice and input as required.
- The policy has been approved and agreed by the Leadership/Management Team and Governing Body (LAB).

- The school has appointed the Designated Safeguarding Lead Mrs Anne Wilson as an appropriate member of the leadership team and the online safety lead.
- The school has appointed Mrs Trudy Hillman as the member of the LAB to take lead responsibility for online safety (e-Safety).
- The online safety (e–Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

1.3 Key responsibilities of the community

Relevant for all settings

All members of school/setting communities have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance.

1.3.1 Key responsibilities of the school/setting management team

Guidance:

The management or leadership team (including the LAB) within a school or setting have statutory responsibilities for child protection, of which online safety is an essential element. KCSiE 2016 highlights a range of specific statutory responsibilities for schools and colleges regarding online safety which governing bodies and proprietors need to be aware of within part two: the management of safeguarding. This includes ensuring that appropriate filtering and monitoring of internet access is in place, that all members of staff receive appropriate training and guidance and that the curriculum prepares children for the digital world.

Additional guidance regarding online safety is provided to schools and colleges within Annex C of KCSiE 2016. Governing bodies and proprietors should ensure that they read Annex C and consider how the requirements can be implemented in their setting.

Management and leadership teams should take steps to consider existing school/setting practice using tools such as the 360 safe tool (www.360safe.org.uk) to ensure that they are aware of the settings current strengths as well as areas for improvement. It is therefore vital that the school/setting management and leadership teams have a sound awareness of online safety issues, and fully understand the importance of having effective policies and procedures in place.

The UK Council for Child Internet Safety Education Group has developed guidance for school governors to help governing boards support their school leaders to keep children safe online. This document can be accessed at: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

The document includes examples of good and outstanding practice, as well as identifying when governors should be concerned. This guidance is non-statutory and should be read alongside the Department for Education's KCSiE statutory guidance. Governors can use this document to:

- gain a basic understanding of the school's current approach to keeping children safe online;
- learn how to improve this approach where appropriate;
- find out about tools which can be used to improve the approach.

The school/setting management and leadership team will have ultimate responsibility for any online safety incidents that may occur whilst on site and lack of knowledge of the issues or technology is no

defence. Leaders and managers must ensure that are aware of safe practice expectations for all member of the community and should seek advice and support both proactively and reactively when developing their online safety approach.

1.3.1 The key responsibilities of the school/setting management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place (Smoothwall) to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies and support as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body (LAB) is identified with a lead responsibility for supporting online safety.
- To ensure that the DSL works in partnership with the online safety e-Safety lead.

1.3.2 Key responsibilities of the Designated Safeguarding Lead (DSL) /online safety lead

Guidance:

All schools and settings are encouraged to appoint an e-Safety or online safety lead, who is responsible for coordinating the whole school/setting online safety approaches, supporting and raising awareness

with the wider community, promoting a safe and responsible online safety culture and acting as the lead for dealing with online safety issues that arise. The online safety lead must have appropriate training, support and authority to carry out the role.

KCSiE 2016 highlights that online safety is a safeguarding concern; therefore the ultimate responsibility for online safety falls within the remit of the DSL. The role of the DSL is to act as a source of support, advice and expertise on all safeguarding issues and encourage a safe and positive culture within the setting and online safety will fall within the scope of this role. Online safety concerns may also cross the child protection threshold and will require referral to other agencies and therefore the online safety lead will require an understanding and experience of this process. It is the role of the DSL to keep appropriate child protection and safeguarding records.

It will not be appropriate for the online safety lead to be another member of staff (e.g. a computing lead or member of the technical staff) unless they have accessed appropriate training, such as that of the DSL to be able to act as a deputy. The online safety lead must be a member of the leadership or management team due to the requirements and expectations of the role (directing resources and advising/supporting other staff) and to ensure that online safety is given a whole setting approach with a coordinated focus.

In some settings another member of staff may be preferred to hold the online safety lead role due to individual knowledge and experience. They should therefore access appropriate training and work in partnership with the DSL who will have overall responsibility for the schools safeguarding approaches. The DSL must always be made aware of and involved with any child protection disclosures or incidents. The DSL must be aware of and involved in all staff online safety training to enable them to keep up-to-date records. The DSL must also be involved in online safety policy development. Staff with appropriate skills, interest and expertise regarding online safety should be encouraged to help support the DSL and any deputies as appropriate, for example when developing curriculum approaches or making technical decisions. However schools and settings must be clear that ultimate responsibility for online safety sits with the DSL

If a deputy DSL takes responsibility for online safety to support the DSL then schools and settings should ensure that sufficient time and resources are in place to enable the DSL to be kept informed on any issues of concerns. Some schools/settings may wish to implement regular safeguarding meetings to allow DSLs time to reflect on the school/settings needs and identify and implement any action as appropriate. Online safety leads do not need to have vast technical knowledge as it is a safeguarding and not a technical role. It is however helpful if the online safety lead has some basic knowledge of current technology and ICT and has a clear understanding of the benefits as well as the risks that technology poses.

Online Safety Groups/Committees

Many schools/settings are now choosing to support the online safety lead by setting up online safety groups or committees who can support and share workloads and tasks. This builds resilience within the setting and enables schools/settings to demonstrate that key members of the community are involved in establishing a shared whole community approach to online safety. Possible online safety group members (subject to individual school/settings needs and requirements) could include:

- DSL(s)
- Computing (IT Lead) Head of Subject
- PSHE Lead/Head of Subject
- Technical staff e.g. Network Manager, IT Technicians

- Governor or board/trust/committee member
- SENCO
- Pastoral staff e.g. Student Support Officer (SSO), learning mentors etc.
- Pupils/children (this may not always be appropriate)
- Other community members (e.g. local Police, Children Centre, Nursery) as appropriate

Online safety groups can be used to support and deliver the key tasks of the online safety lead and are a useful approach to help enable incorporate and maximum the range of experiences and expertise within schools/settings. The group should report regularly to the governing body or other appropriate body to help inform them of existing practice and localised concerns.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms (these will be logged on CPOMS).
- Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other related procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety

1.3.3 Key responsibilities of staff

Guidance*:*

All members of staff play an essential role in creating a safe culture within settings, both on and offline. All members of staff should seek to promote safe and responsible online conduct with and by children as part of the curriculum and as part of their safeguarding responsibilities. All members of staff will need to role model positive behaviours when using technologies, either directly with children or in the wider context. All staff should be aware of and ensure they adhere to the school/setting Acceptable Use Policies (AUPs).

Children will come into contact with a variety of staff throughout their time in education. Members of staff in schools and settings are likely to be the first point of contact for online safety incidents, or will be in a position to identify changes in behaviour which may indicate that an individual is at risk of harm. It is therefore essential that all members of staff have a good awareness of online safety issues, KCSiE 2016 highlights that all staff in schools and colleges must be aware of online safety concerns including, but not limited to sexting and cyberbullying. All members of staff must also know the appropriate procedures for escalating incidents or concerns to the DSL and also to external agencies as appropriate. All members of staff must be made aware of the duty to respond, report and record safeguarding issues and therefore be aware of the schools procedures for managing on and offline safety disclosures or concerns.

Where services are provided within schools/settings by external contractors, it is essential that the school takes steps to ensure that outside providers support the schools online safety ethos and will adhere to the settings online safety policy and practices.

1.3.3 The key responsibilities for all members of staff are:

- E Contributing to the development of online safety policies.
- E Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- E Taking responsibility for the security of school/setting systems and data.
- E Having an awareness of a range of online safety issues and how they relate to the children in their care.
- E Modelling good practice when using new and emerging technologies
- E Embedding online safety education in curriculum delivery wherever possible.
- E Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- E Knowing when and how to escalate online safety issues, internally and externally.
- E Being able to signpost to appropriate support available for online safety issues, internally and externally.
- E Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- E Demonstrating an emphasis on positive learning opportunities.
- E Taking personal responsibility for professional development in this area.

1.3.4. Additional responsibilities for staff managing the technical environment

Guidance:

Members of staff who are responsible for managing the school/setting technical environment have an essential role to play in establishing and maintaining a safe online environment and culture within establishments.

Staff with responsibility for the technical environment should work closely with the school leaders, online safety coordinator, DSL as well as pastoral and curriculum staff (where appropriate) to provide expertise relating to education use of IT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.

Technical staff will need clear supervision and support in their roles by the leadership and management team (including safeguarding leads) and, along with all staff, will require regular training and professional opportunities to enable them to remain up-to-date with emerging online safety issues.

Technical staff should be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL and/or headteacher/manager in line with existing school/setting safeguarding policies (including allegations and whistleblowing).

In some settings, technical support may be outsourced to an external service provider. In such instances, it is important that the service provider understands supports and upholds the settings online safety practices, taking appropriate steps to minimise risks, and reporting any breaches of system or network security to online safety coordinator and leadership team to enable appropriate internal action to be taken.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's IT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 Key responsibilities of children and young people

Guidance:

The essential role and responsibilities for children and young people themselves in relation to their own online safety should not be underestimated. Children should be encouraged and empowered to develop safe and responsible online behaviours over time which will enable them to manage and respond to online risks as they occur.

Children and young people should form an important part of policy development, especially with regards to safeguarding, as if children feel that their views have been heard (and in turn can therefore understand some of the issues affecting the decisions) then they may be more inclined to abide by them.

It should also be understood that children are more likely to be aware of and understand new developments within technology and may be able to provide schools and settings with an excellent way of keeping up-to-date with the rapidly changing pace of development, especially within social media and the associated apps and games.

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers

Guidance:

Parents /carers play a crucial role in developing children's safe and responsible online behaviours, especially where a majority of children's access will be taking place when they are not on the school/setting site. Schools and settings have a clear responsibility to work in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help schools/settings to reinforce online safety messages and promote and encourage safe online behaviours wherever, and whenever, children use technology.

A partnership approach will need to be established via a variety of approaches and strategies and schools and settings should ensure that online safety messages are shared and promoted with parents through a variety of communication channels and events throughout the year.

As with children and young people, parents/carers should be involved in the development of the online safety policies to help build and develop a shared approach to safeguarding children online, both at school and at home.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

Schools and settings will be using a variety of online communication and collaboration tools both informally and formally with children, parents/carers and staff. It will be important that managers and leaders are aware of this use and provide clear boundaries and expectations for safe use.

2.1 Managing the school/setting website

Relevant for settings who maintain a website

Guidance:

Many schools and settings have created excellent websites that share essential information with the community and also inspire children to create and celebrate work of a high standard. Websites can be used to give members of the community information about policies, procedures and local events and can also be used to celebrate children's work, promote the school/setting and publish resources for projects. Editorial guidance will help reflect the settings requirements for accuracy and good presentation.

For some settings, especially early years providers, an online presence may take place through social media channels rather than via formal website. Settings should therefore access section 3 of this document regarding social media, to ensure that this is done safely and responsibly.

Publication of information should be considered from a personal and school/setting security viewpoint. Sensitive information about schools/settings and children could be found in a newsletter but a website is more widely available to the public. Material such as detailed school plans and full staff contact details may be better published in the staff handbook or on a secure part of the website which requires authentication from visitors.

Schools are required to publish certain information online – this means that they **must** have a website. The most recent guidance reading information that must be published online can be found here (gov.uk) What Maintained Schools Must Publish Online

Statements:

- E The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- E The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- E The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- E The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- Pupils work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

Discussion:

Still and moving images and sound add liveliness and interest to a publication, display or website, particularly when children can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of children's names with their images is not acceptable by educational settings. Images of a child must not be published without the parent's or carer's written permission. Some schools/settings ask permission to publish images of work or appropriate personal photographs on entry, some once a year, others at the time of use.

For further information please see: (East Sussex) ICT E-safety Online Safety Education

Statements:

- E The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- E The school/setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- E In line with the image policy, written permission from parents or carers will always be obtained before images/videos of individual pupils are electronically published.

2.3 Managing email

Relevant for all settings

Guidance:

Email is an essential method of communication for staff, parents and children. The implications of email use for the school/setting need to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to the school/setting community that bypass traditional boundaries and therefore use of personal email addresses by staff for any official business should not be permitted.

Schools and settings need to address the concern regarding the degree of responsibility that can be delegated to individuals, as once email is available it is difficult to control. In the school /setting context (as in the business world), email should not be considered private and most schools/settings reserve the right to monitor official email communication. There is however a balance to be achieved between necessary monitoring to maintain the safety of the community and the preservation of employees human rights, both of which are covered by recent legislation.

Schools will need to consider and manage children's use of school provided email addresses. The use of email identities such as ***john.smith@school.e-sussex.sch.uk*** may need to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided if they can be used to identify both a pupil's full name and their school. Schools will need to consider if it is appropriate for pupils to have access to an email address which allows them to communicate externally. Secondary schools should limit pupils to email accounts which have been approved and are managed by the school and for primary schools, whole-class or project email addresses may be more appropriate.

When using external email providers, such as Google Apps for education, to provide staff and pupils with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services. Schools must ensure that they abide by data protection legislation and are consciously aware where that information is physically and/or virtually stored and how it may be accessed. Schools will need to ensure that any use of specific systems such as Google Apps for education etc. are appropriately risk assessed and will need to include their use within acceptable use policies.

Spam, phishing and virus attachments can make email dangerous. The East Sussex Education Network uses industry leading email relays to stop unsuitable mail using reputation filtering for schools that manage their own email servers in house. Currently about 95% of email is rejected as spurious. Schools and settings should consider security steps required to reduce these risks. Many schools are now using cloud provided email services (e.g. Microsoft Office365 or Google Mail) which also include such filtering systems as standard. Heron Park primary Academy uses Microsoft Office365.

Professionals must ensure that their use of email at work always complies with data protection legislation and confidential or personal data must not be sent electronically via email unless they are appropriately encrypted. In most cases simply using a password to protect file attachments will not be sufficient and can breach data protection requirements. Leaders are strongly encouraged to ensure staff are appropriately trained and should ensure members of staff use appropriately secure email systems to share any sensitive or personal information.

2.3 Statements:

- E Pupils may only use school/setting provided email accounts for educational purposes
- E All members of staff are provided with a specific school/setting email address to use for any official communication.
- E The use of personal email addresses by staff for any official school/setting business is not permitted.
- E The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- E Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- E Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- E Whole -class or group email addresses may be used for communication outside of the school .Excessive social email use can interfere with teaching and learning and will be restricted.
- E Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- E School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

Relevant for all settings who use video conferencing and webcams

Guidance:

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Equipment ranges from small PC systems (web cams) to large room-based systems that can be used for whole classes or lectures.

The National Educational Network (NEN) is a private broadband, IP network interconnecting the ten regional schools' networks across England with the Welsh, Scottish and the Northern Ireland networks.

Schools with full broadband are connected through the East Sussex Education Network (ESEN) and have access to services such as gatekeepers and gateways to enable schools to communicate with external locations. Schools may also decide to use conferencing services such as Skype for education and Flashmeeting which do not require ESEN systems.

If Flashmeeting is used, conferences should always be booked as private and not made public. The conference URL should only be given to those who you wish to take part. Check who has signed into your conference; as a guest without a camera would not be visible.

Video conferencing introduces exciting dimensions for educational contexts; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet and allow children to explore and source new experiences. The availability of live video can sometimes increase safety — you may believe that you can see who you are talking to — but if inappropriately used; a video link could reveal security details, place staff at risk or be used to exploit and abuse children.

Please be aware that use of webcams for CCTV would need to be highlighted within the school/setting image policy.

For further information please see: (East Sussex) School Management School Policies Data Protection CCTV

2.4 Statements:

- **E** The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- **E** All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- **E** Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- **E** Videoconferencing will be supervised appropriately for the pupils' age and ability.
    - No child/group of children will be left unattended at any point during the videoconference.
- **E** Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.

- E Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet (and associated devices)

Relevant for all settings that provide internet access for children

Guidance:

Increased use of internet enabled devices and improved Internet access and its impact on pupils learning outcomes must be considered by leaders and managers. Developing safe and effective practice in using the Internet for teaching and learning is essential.

Schools and settings will need to adapt this section in accordance with the internet access provided as well to identify safe approaches for the full range of devices used, for example tablets. If schools/settings use devices which do not require pupils or staff to “login” to systems (such as iPads) to access the internet then leaders/managers must ensure that there is appropriate mechanisms in place to log which member of the community has had access to which devices in order to ensure that if concerns are identified, the school can trace users.

The decision regarding which classroom tools, such as search engines, to use will be down to individual schools (Headteachers and Governing bodies) to consider. Increasingly many schools are choosing to allow children (from upper key stage two onwards) to use popular search engine sites such as Google or Bing rather than tools specifically considered to be “child friendly”. Schools should be aware that using tools such as Google and Bing does increase the risks of children being exposed, both accidentally and deliberately to unsuitable content. However this decision should be taken following a consideration of both the strengths and risks to children’s learning if they are unnecessarily restricted from online resources. It is likely that this decision will depend on the children’s ages and abilities and also adult supervision and any use of monitoring systems.

These decisions should be made by headteacher and leaders, based on a risk assessment approach which considers the benefits of access for education and learning, the possible safeguarding concerns and also the possible negative impact on pupil’s education

All members of staff must be aware that no search engine or filtering tools is ever completely safe and appropriate supervision, use of safe search tools (where possible), pre-checks of search terms, age appropriate education for pupils and robust classroom management must always be in place. However

despite these steps children may still be exposed to inappropriate content therefore leaders must ensure that there are clear procedures for reporting access to unsuitable content, which are known by both children and staff.

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read and a whole curriculum approach may be required. Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating Internet content, for example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of. Additionally, the potential risk of exposure to extremist content when researching some content must also be considered.

2.5 Statements:

- **E** Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access curriculum policies for further information.
- **E** The school/setting's internet access will be designed to enhance and extend education.
- **E** Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- **E** All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- **E** Supervision of pupils will be appropriate to their age and ability
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- **E** All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
    - School owned devices will be handed in and monitored regularly (2 x yearly) and any issues dealt with according to the procedures set out in the AUP.
- **E** Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- **E** Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- **E** The school will use age appropriate search tools ***(Google)*** as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- **E** The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of school learning platforms/portals/gateways

Relevant for any settings that have a learning platform/portal/gateway

Guidance:

An effective learning platform or environment can offer schools and settings a wide range of benefits to staff, children and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work. The Learning Platform/Environment (LP) must be used subject to careful monitoring by the Leadership Team. As usage grows then more issues could arise regarding content, inappropriate use and behaviour online by users. Leaders have a duty to review and update the policy regarding the use of the Learning Platform, and all users must be informed of any changes made.

2.6 Statements: Heron Park Primary Academy uses DB Primary as its Learning Platform.

- E Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- E Pupils/staff will be advised about acceptable conduct and use when using the LP.
- E Only members of the current pupil, parent/carers and staff community will have access to the LP.
- E All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- E When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

Guidance:

Schools and settings should acknowledge that there are significant potential benefits for communication, engagement, collaboration and learning via the Internet and social media. However schools also need to recognise that there are several risks associated with users (staff, pupils and the wider school community) especially when accessing and handling information as part of official school/setting business.

Adults and children need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social media tools can connect people with similar or even very different interests. Users can be invited to view personal spaces and content and leave comments, over which there may be limited control. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, video/photo sharing, chatrooms, instant messenger and many others. Examples of popular sites currently include Facebook, Instagram, SnapChat, Twitter, YouTube and Instagram but these sites are constantly changing and naming specific sites within the policy may cause misinterpretation and should be avoided unless schools/settings have official social media channels.

For responsible children and adults, social media provides easy to use, free facilities, which enable them to communicate with friends and family. However some social media sites and apps are only free to use due to advertising and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information to social media sites as well as being made aware of the associated benefits. Pupils should be made aware of the potential risks of social media such as advertising, scams, and contact from strangers and the difficulty of removing an inappropriate image or information once published.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, Instagram, SnapChat, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible when using most popular forms of social media.

Clear guidance will be required to ensure that schools and settings are not exposed to legal risks, that reputation of schools/settings is not adversely affected, that users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school/setting and to ensure that all members of communities are safeguarding from harm (both on and offline).

The following content may not be required by all schools/settings. Some settings may choose to use section 3.1 only and some settings may find it more appropriate to create a separate and specific social media policy.

3.1. General social media use

Relevant for all settings

3.1. Statements:

E Expectations regarding safe and responsible use of social media will apply to all members of Heron Park Primary Academy community and exist in order to safeguard both the school/setting

and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of Heron Park Primary Academy community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Heron Park Primary Academy community.
- All members of Heron Park Primary Academy community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school/setting will control pupil and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- The use of social networking applications during school hours for personal use **is not** permitted.
- Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Heron Park Primary Academy community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, behaviour, safeguarding and child protection including the allegations against staff section.

3.2. Official use of social media

Relevant for all settings that use social media officially as a communication channel.

Guidance:

Schools/settings may wish to highlight within this section the specific action that will be taken to ensure safe and responsible use of the official social media accounts, for example what privacy settings will be used, how follow/join requests will be managed, if private messages will or will not be permitted etc. Schools and settings are encouraged to undertake an appropriate risk assessment prior to use and to discuss safe practice regarding official use of social media.

3.2 Statements:

- *Heron Park Primary Academy* official social media channels are:
  - ***. Twitter link, Facebook page link.***
- Official use of social media sites by the school/setting will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher and Social Media Manager (Yvonne Streeter).
- Official school/setting social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school/setting provided email addresses to register for and manage any official approved social media channels.

- E Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- E All communication on official social media platforms will be clear, transparent and open to scrutiny.
- E Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- E Official social media use will be in line with existing policies including anti-bullying and child protection and safeguarding.
- E Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- E Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- E Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.
- E Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- E Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school/setting will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school/setting website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school/setting will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff personal use of social media

Relevant for all settings

Discussion:

'Keeping Children Safe in Education' 2016 highlights that Governing Bodies and proprietors need to ensure that their settings have "…a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include – acceptable use of technologies, staff/pupil relationships and communications including the use of social media." It is therefore essential that schools ensure all members of staff are aware of professional boundaries regarding both their 'on' and 'offline' communication.

Schools and settings must be aware they cannot ban members of staff from using social networking sites in their own personal time; however they can and should provide advice for staff and put in place appropriate guidance and boundaries around interaction with current and past pupils and parents/carers. All members of staff should be made aware of the potential risks of using social networking sites or personal publishing both professionally and personally. Members of staff should be made aware of the importance of considering the material they post online and the need to ensure that their personal profiles are secured or set to private. All members of staff should be made aware that publishing

unsuitable material online may affect their professional status and reputation and bringing the school or profession into disrepute is a disciplinary issue.

School/setting leaders and managers should ensure that all members of staff are aware of the school/setting policy regarding communication with pupils and parents via social media. Leaders should be aware that it is recommended that all members of staff should be advised not to communicate with or add as 'friends' any current or past pupils, or current or past pupils' family members via personal social media sites, applications or profiles.

A commonplace practice of staff adding current and ex-pupils and parents as "friends" on personal social networking sites has been highlighted within several serious case reviews for both schools and early year's settings as a possible indicator of an unsafe culture. If unchallenged, this practice can potentially blur professional boundaries between staff, parents and children and can also undermine the wider communities' abilities to identify and raise concerns regarding any inappropriate professional conduct. An analysis of National College of Teaching and Leadership (NCTL) hearings in 2014 identified that the number of teachers banned for inappropriate use of social media has more than doubled, with a number of cases involving sexual relationships with current or ex-pupils. Whilst the vast majority of social media communication between staff and members of the community is unlikely to deliberately abusive, leaders must ensure that boundaries regarding online communication are made clear and that all members of staff are aware of what the school consider to be acceptable and unacceptable behaviour and communication online.

Many members of staff will add current and ex-pupils as friends with good intentions, for example offering support, or keeping in touch with them through the next stages of their life. Even though members of staff may feel that they can keep themselves safe and trust the integrity of current and ex-pupils or parents/carers by accepting such requests, staff could be putting themselves in a vulnerable position. By adding ex or current pupils or parents/carers, members of staff could be at risk of sharing personal information such as photos or comments which can be misinterpreted and shared without their knowledge or consent.

Adding ex or current pupils as friends may also mean that members of staff have access to personal information about pupils or parents which could lead to possible concerns, for example if pupils or parents post unsuitable content or material. By adding ex-pupils, members of staff can be at risk of undermining their professional reputation, as ex-pupils may have friends or other family members who are still pupils at the school. Members of staff who add current or ex-pupils or parents/carers may be potentially be leaving themselves open to allegations of inappropriate contact or conduct and could risk being exposed to unwanted contact and harassment from others.

There is no legal age or precedent whereby it becomes 'acceptable' for staff to add ex-pupils onto personal social networking sites. It is not good practice for any members of staff to add current or ex-pupils or parents/carers as friends (unless there is a pre-existing relationship) in order to safeguard themselves from allegations and also to maintain professional boundaries. Many leaders and managers have chosen to implement their own recommendation for staff (typically stating that staff must not add ex-pupils until they are classed as adults and have left the school for at least 2/3 years e.g. are now aged 18, or 21 if there is a sixth form) however this decision will come down to the schools own risk assessments and will be based on their individual community. One risk with providing a limit for acceptance could be that the school might be viewed as condoning the behaviour, which could lead to concerns about possible breaches of trust or professional boundaries becoming blurred.

The best approach is to promote a transparent relationship between staff and the designated safeguarding lead. If ongoing contact with children is required once they have left the school, for

example to celebrate success, then it is recommended that leaders encourage the use of official existing alumni networks or official social media channels , or for staff to use their official communication tools, such as their school email address. This ensures that all communication is transparent and open to scrutiny and will safeguard staff from allegations.

Any pre-existing relationships or exceptions between current or ex-pupils or parents which may compromise a member of staffs' ability to comply the schools policy (for example their own children are pupils, or a parent is a family member or friend) must be discussed between the member of staff and the DSL and/or manager/headteacher. This will ensure that the relationship is formally acknowledged and will enable the manager/headteacher to discuss the schools expectations regarding professional conduct clearly with the member of staff.

The following links may be helpful to share with members of staff:
(childnet.com) Teachers and Professionals - for you as a professional
(childnet.com) Teachers and Professionals Professional Reputation
(saferinternet.org.uk) Teachers and Professionals Professional Reputation

Some schools/settings may wish to highlight the policy regarding this within the Acceptable Use Policy rather than with a separate policy.

3.3 Statements:

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school/setting Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or a member of the of Leadership Team/headteacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Staff will not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.
- Any communication from pupils/parents received on personal social media accounts will be reported to the designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff are encouraged not to identify themselves as employees of Heron Park Primary Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and also to safeguard the privacy of staff members and the wider community.
- Member of staff will ensure that they do not represent their personal views as that of the school/setting on social media.
- School/setting email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school/settings social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 Staff official use of social media

Relevant for all settings

Guidance:

This section will be relevant for settings whereby members of staff run or contribute to school official social media channels, for example a whole school Facebook page or a departmental Twitter account.

3.4 Statements:

- If members of staff are participating in online activity as part of their capacity as an employee of the school/setting, then they are requested to be professional at all times and that they are an ambassador for the school/setting.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school/setting.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher/manager of any concerns such as criticism or inappropriate content posted online.

- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the social media Acceptable Use Policy.

3.5 Pupils' use of social media

Relevant for all settings but will need to be adapted according to the age and ability of children

Guidance:

Social media is now an everyday form of communication for many children and young people and forms a vital part of growing up in today's modern Britain and the wider global society. Whilst many schools and settings will choose to block access to social media sites for children using official systems and equipment, it cannot be assumed that they will not access them offsite or when using personal devices. It is therefore essential that children and young people are given age appropriate education regarding safe and responsible use and are also appropriately exposed to social media sites to enable them to develop and build skills and resilience. This approach must be considered in conjunction with other relevant policies, for example with regards to curriculum, filtering and monitoring.

Schools and settings should be aware that many popular social media services such as Facebook, Instagram, Twitter and YouTube have age restrictions of 13+. This limit is however not a legal limit, for example it is not a criminal offence for a child (or indeed a parent) to lie about their age in order to set up an account. The age limit is put in place due to the Children's Online Privacy and Protection Act (COPPA) legislation and is there to protect children's privacy and to prevent them being targeted with unsuitable advertisements. Social media sites cannot guarantee that content posted on them is suitable for children as many of them are not moderated and as such the recommended approaches for child safety are not always in place.

It is very important for schools and settings to recognise that if we simply ban children from using social media (especially if they are under 13) and do not discuss safe behaviour, then many of them will be using popular social media sites and will not be receiving appropriate advice or support. This could possibly place them at increased risk of harm, as children may be more likely to lie about and hide their online behaviour and may not disclosure concerns for fear of being punished. Schools and settings should consider the most appropriate way to respond to social media use and this is likely to vary according to the age of the children and the possible safeguarding risks. When schools and settings are made aware of underage social media use then the designated safeguarding lead should speak directly to all children and parents involved in order to share their concerns and ensure that appropriate action is taken. In some cases schools and settings could consider reporting accounts to social media sites for removal; however leaders must be aware that this may not always resolve the problem as pupils may be able to create additional accounts. Education for all members for the community about safe use of social media is therefore essential.

If specific concerns regarding pupils' use of social media are bought to the schools or settings attention then leaders/Headteachers should ensure that they are formally recorded along with any action taken. If children are using social media sites inappropriately (such as cyberbullying, posting personal

information, adding strangers as friends etc.) or there are other safeguarding concerns due to vulnerabilities etc., then the school/setting should respond to the concern in line with existing policies, for example anti-bullying, child protection and safeguarding or behaviour policy. If a child is at risk of serious harm then the DSL must be informed and the existing child protection procedures should be followed.

3.5 Statements:

- E Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- E Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- E Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- E Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- E Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- E Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- E Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- E Any official social media activity involving pupils will be moderated by the school where possible.
- E The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- E Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- E Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

Relevant for all settings

Guidance:

Mobile phones and other personal devices such as tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops are considered to be an everyday item in today's society and even children in early years settings may own and use online personal devices regularly. Mobile phones and personal devices can be used to communicate in a variety of ways with texting, cameras, voice recording and internet accesses all common features.

However, mobile phones and personal devices can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render children or staff subject to online (cyber)bullying;
- Internet access on phones and personal devices can allow children and adults to bypass security settings and filtering;
- They can undermine classroom discipline as they can be used on "silent" mode;
- If used to access school data then they can breach data protection and confidentially policies;
- Mobile phones and devices with integrated cameras and other recording systems could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff.

Under the EYFS, section 3.4 all settings and foundation stage providers must have a clear safeguarding policy which covers the use of mobile phones and cameras in the setting. It is advisable that this policy is extended to cover the wide range of devices now available, such as tablets, phones etc. It is also advisable that all education settings have a clear and robust policy which covers specific expectations for safe and responsible use for mobile phones and personal devices by children, staff and others. Some settings may choose to create a separate policy regarding mobile phones and personal devices.

A policy which totally prohibits children, staff or visitors from having mobile phones or personal devices when on site could be considered to be unreasonable and unrealistic for schools and settings to be able to achieve. For example many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone and many staff and visitors use mobile phones to stay in touch with family.

Due to the widespread use of a range of internet enabled personal devices, it is essential that schools and settings take steps to ensure all mobile phones and personal devices are used responsibly and it is essential that staff and children use of mobile phones and devices does not impede teaching, learning and good order. Staff should be given clear boundaries on professional use and expectations, especially regarding role modelling safe behaviour and ensuring classroom management. Learners should be given explicit education regarding appropriate use of mobile phones and personal devices in accordance with their own age and ability as well as developing a clear understanding of the schools expectations and any sanctions for misuse. The decision regarding the use of mobile phones and personal devices is a school/setting decision to be made, however the following points have been provided to support schools and settings in creating effective policies.

Headteachers, Governing bodies and managers will need to consider possible risks and concerns which could arise as a result of allowing staff to use personal devices for official business e.g. to receive work email automatically on their personal devices. This is especially a concern with regards to possible data

protection and confidentiality breaches, for example if a personal device is lost or stolen or shared with family members. Headteachers, Governing bodies and managers must implement appropriate strategies with staff to reduce risk if this practice is permitted. This could include implementing appropriate encryption and authentication (for example staff logging into email via a web client), highlighting safe practice within Acceptable Use Policies and identifying concerns via staff training and induction.

Schools/settings which elect to allow members of the community to use their own devices for educational use within the classroom should create a separate and specific policy covering the expectations and requirements for safe and responsible use. The National Education Network (NEN) has some links and information regarding this approach: National Education Network - bring your own device (BYOD)

Headteachers, managers and leaders should implement a robust risk assessment to explore both the benefits and risks the use of personal devices to ensure that a proportional and realistic policy decision is made. Where possible parents, children and staff should be included within this process in order to increase engagement and develop whole school/setting ownership of the policy. The decisions should be supported with robust training and an appropriate acceptable use policy which is appropriate to the decision and clearly states expectations for safe use as well as sanctions for misuse.

4.1 Rationale regarding personal devices and mobile phones

4.1 Statements:

- E The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members Heron Park Primary Academy community to take steps to ensure that mobile phones and personal devices are used responsibly.
- E The use of mobile phones and other personal devices by young people and adults will be decided by the school/setting and is covered in appropriate policies including the school Acceptable Use Policy
- E Heron Park Primary Academy recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

4.2 Expectations for safe use of personal devices and mobile phones

4.2 Statements:

- E All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies - AUP
- E Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school/setting accepts no responsibility for the loss, theft or damage of such items. Nor will the school/setting accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- E Mobile phones and personal devices are not permitted to be used in certain areas within the school/setting site such as changing rooms, toilets and swimming pools.
- E The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- E Members of staff will be issued with a school/work phone number and email address where contact with pupils or parents/carers is required.

- E All members of Heron Park Primary Academy community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- E All members of Heron Park Primary Academy community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Heron Park Primary Academy community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
- School/setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School/setting mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

Guidance:

This section will need to be adapted according to the school/settings specific policy decisions. Leaders and mangers should list the specific expectations regarding children and young people's safe use of mobile phones and personal devices e.g. Mobile phones and devices must be kept securely in a locker, or locked in a secure place in the school office.

Consideration will need to be given by schools regarding safe and appropriate use of personal devices by pupils even when they have access to devices which are not internet enabled, for example personal laptops, tablets, games consoles and MP3 players such as the iPod touch. Many settings will believe that if they do not facilitate access to the internet or the children's own devices do not have built in 3/4G access then there is no possible risk, however this is not the case. For example taking and sharing indecent or inappropriate images can occur on any devices with inbuilt cameras, even if there is no internet access and this can place pupils at risk of serious harm. Even if schools decide to attempt to completely "ban" pupils use of mobile phones and personal devices, education about safe and appropriate use must still be provided within the curriculum.

Schools and settings may wish to cover pupils' personal use of devices within other policies such as the Acceptable Use Policy and behaviour policy etc. Schools/settings should ensure that their policies regarding confiscation, screening and searching are up-to-date and are clearly communicated to all members of the community, including pupils and parents. The Department for Education has guidance available for headteachers here: (gov.uk) Searching Screening and Confiscation The SWGfL has a template Search and Deletion Policy which schools may wish to access and adapt (swgfl.org.uk) Creating an E-safety Policy

For settings with residential provision, such as boarding schools or residential special schools, then considerations must be given as to how the school can balance the need and importance of internet use for children to be able to take part in age appropriate peer activities, including staying in touch with friends and family but balanced with the need for the school to be able to detect abuse, bullying or unsafe practice by children. Residential Schools and settings must ensure their policies explicitly cover how the school will monitor and regulate children's use of the internet, including via personal devices, out of school hours. Parental consent should be considered along with the views of the children. Residential

settings should be mindful of their responsibilities with regards to the national minimum standards (NMS) for their organisation.

4.3 Statements:

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Pupil's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during the school day.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the SLT.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school/setting phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office – there will be no exceptions.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the schools policy. **-** ***See*** (gov.uk) Searching Screening and Confiscation.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices and mobile phones

Guidance:

This section will need to be adapted according to the school/settings specific policy decisions. Within this section leaders and managers should list their specific expectations regarding safe use of staff personal mobile phones and devices e.g. Mobile phones and devices must be kept securely in a locker, locked draw or other secure place.

Leaders should be aware that seizing and searching members of staffs' personal devices may be unlawful. If leaders feel this is required or appropriate, for example if a criminal offence may have been committed, then the appropriate agency should be informed. The DSL may wish to seek advice from the Local Authority Designated Officer (LADO) or the SLES Safeguarding team if there has been an allegation against a member of staff.

Leaders and managers should also identify school expectations regarding appropriate and proportional staff use of personal devices to access school content e.g. school email, learning platforms and should identify expectations for safe use to ensure possible risks can be mitigated. This may include using password protected webmail clients, encryption etc.

4.4 Statements:

- E Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- E Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- E Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- E Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the SLT in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management section in the safeguarding and child protection policy.

4.5 Visitors' use of personal devices and mobile phones

Guidance:

This section will need to be adapted according to the school/settings specific policy decisions.

4.5 Statements:

- E Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy.
- E Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

Relevant for all settings

Guidance:

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems and can offer significant benefits for learning, communication, engagement and participation as well as potential hazards. The safest approach is to deny access until a risk assessment has been completed and safety and appropriate action has been established and taken.

New applications are continually being developed and changing which can offer immense opportunities for socialisation and learning as well as increasing dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Schools, settings, leaders and managers will need to keep up to date with new technologies, including those relating to mobile phones personal devices, and be ready to develop appropriate strategies. For instance instant messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate an absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact pupils and therefore a school owned phone or communication channel should be issued.

The inclusion of inappropriate language, behaviour or images online can often be difficult for staff to detect and robust classroom management with appropriate training and support will be required for all members of staff.

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school/setting will need to address the fact that it is not possible to completely remove the risk that children might access unsuitable materials via the school/setting system. It is wise to include a disclaimer, an example of which is given below.

Risks can be considerably greater where tools are used which are beyond the schools control such as most popular social media sites.

5.1 Statements:

- E Heron Park Primary Academy is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- E Emerging technologies will be examined for educational benefit and the SLT will ensure that appropriate risk assessments are carried out before use in school is allowed.
- E The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. (Smoothwall Filtering)
- E The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always

possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.

- E The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school leadership team.

5.2. Internet use throughout the wider school/setting community

Relevant for all settings

Guidance:

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, café, restaurant, adult education centre, village hall or supermarket. Ideally, young people would encounter a consistent internet use policy wherever they are. There is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access.

Although policies and practice may differ, community partners should adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful.

5.2 Statements:

- The school will liaise with local organisations to establish a common approach to online safety (e–Safety).
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

5.3 Authorising internet access

Relevant for all settings who facilitate internet access

Guidance:

The school/setting should allocate Internet access to staff and children on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school or early years setting, children's internet usage should be fully supervised.

Normally most children will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental awareness should be encouraged for Internet access in all cases — a task that may be best organised annually when children's home details are checked and as new children join or as part of the Home-School/setting agreement. If schools/settings do request parental consent for

internet access it is essential to record this data. Schools must be aware that pupils should not be prevented from accessing the internet unless the child is subject to a sanction as part of the school behaviour policy.

5.3 Statements:

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

Relevant for all settings

Guidance:

Online safety forms an important part of the Computing curriculum programmes of study for children within schools and this highlights the importance for children to use technology safely and respectfully, understand how to keep personal information private and be able identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies from an increasingly early age. Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Critical awareness of the dangers and consequences of plagiarism, copyright, piracy, reliability and bias will need to be explored. Children will need to develop an understanding on how to become safe and responsible online or digital citizens and this should be developed within an appropriate Personal Social and Health Education (PSHE) curriculum.

Whilst the Computing curriculum will form an essential part of online safety education for children and young people, safe and responsible use of technologies must be embedded throughout the whole school curriculum to ensure children develop the required range of digital literacy and safety skills as well as to develop online resilience to enable them to become safe and responsible internet users.

Keeping Children Safe in Education 2016 has highlighted that governing bodies and proprietors need to '*…ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum which may include covering relevant issues through personal, social, health and economic education (PSHE), tutorials (in FE colleges) and through sex and relationship education (SRE)*' (Section 68).

It is therefore essential that educational settings give consideration as to the most appropriate place within the curriculum for teaching online safety (e-Safety). Whilst this could be as part of the computing curriculum or a special event or assembly, best practice is where schools develop and implement a whole school and progressive curriculum which allows pupils to develop over time, appropriate strategies to respond to risk. Online safety education must also be reinforced whenever pupils are using the internet, therefore a computing online approach will not be sufficiently robust.

Useful online safety (e-Safety) programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Digital Literacy Scheme of Work: www.digital-literacy.org.uk
- Internet Matters: www.internetmatters.org
- BBC
    - www.bbc.co.uk/webwise
    - www.bbc.co.uk/cbbc/topics/stay-safe
    - www.bbc.co.uk/education

Other suggested links can be found in Appendix C of this document.

Many pupils are very familiar with culture of mobile and Internet use and it is wise to involve them in designing the school online safety (e-Safety) policy, possibly through a pupil council. As pupils' perceptions of the risks will vary; the online safety (e-Safety) rules may need to be explained or discussed and communicated in a variety of different formats.

6.1 Statements:

- E An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- E Education about safe and responsible use will precede internet access.
- E Pupils' input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- E Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- E All users will be informed that network and Internet use will be monitored (Smoothwall Monitoring System.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

6.2 Engagement and education of children and young people who are considered to be vulnerable

Relevant for all settings

Guidance:

Children and young people may be considered to be vulnerable for a variety of reasons. This could include children with special education needs, children with mental health needs, children in care, children who have experienced trauma and abuse, children with low self-esteem, children with English as an additional language etc. Children may also be considered to be vulnerable on a temporary basis for example those experiencing hardship. Whole school/setting strategies should be established in order to protect a wide cohort of children and young people and will need to be able to support the individual needs that vulnerable pupils may display.

6.2. Statements:

- E Heron Park Primary Academy is aware that some children may be considered to be more vulnerable online due to a range of factors.
- E Heron Park Primary Academy will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENDCo, SSO).

6.3 Engagement and education of staff

Relevant for all settings

Guidance:

Annex C of Keeping Children Safe in Education 2016 highlights that governors and proprietors should ensure that as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training on a regular basis. It is recommended that online safety training is revisited as part of safeguarding training for all staff and it is important that leaders and managers attend, facilitate and support training to ensure the online safety culture is clearly established and implemented. It is important that online safety training for staff is not just provided as a reactive approach following concerns and should become a regular feature of staff training and development.

Many schools/settings choose to provide at least annual updates as part of whole staff training due to the rapid pace of change of technology to ensure that all staff understand how to protect both children and themselves as professionals. Induction of new staff should always include a discussion about the online safety (e-Safety) policy and Acceptable Use policy.

It is important that all members of staff feel confident to use new technologies in teaching and the online safety (e-Safety) policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school/setting which may be accessed outside of the school/setting network. Schools/settings must be clear about the safe and appropriate uses of their equipment and have rules in place about use of the equipment by third parties (for example devices are not shared with family members). Staff must be made aware of their responsibility to maintain confidentiality of school/setting information.

6.3 Statements:

- **E** The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.

- E Staff will be made aware that our Internet traffic can be monitored and traced to the individual user (Smoothwall Monitoring System). Discretion and professional conduct is essential when using school systems and devices.
- E Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular (at least annual) basis.
- E All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or monitor IT use will be supervised by the SLT and will have clear procedures for reporting issues or concerns.
- The school/setting will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

Relevant for all settings

Guidance:

Parents and carers form a vital element in the approach to teaching and empowering children to become safe and responsible digital citizens.

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. Technology can sometimes be seen as a "scary" or "frightening" issue to many adults and using the words such as "IT" and "Technology" can sometimes put parents/carers off attending Online Safety events as they may be concerned about not having sufficient computer skills to help protect their child. Online safety or "e-Safety" is not about technology skills, it is about keeping children safe online and so parenting skills and communication and not computing/technology are the most important thing.

Sometimes families may think they are doing enough to protect their children by putting filters on search engines, installing antivirus software, having a laptop downstairs and banning children from using certain sites without considering how successful these tools are or if their children could access the internet elsewhere, so it is important to highlight that discussion and education about safe use is the key.

It is important that schools/settings focus on the importance of keeping children safe online and that online safety is not seen as a purely IT issue. By working together, parents and carers, schools/settings and other professionals can help to reinforce online safety messages and can encourage positive behaviour wherever and whenever children go online.

Awareness-raising with families should focus on:

- The range of different ways children and young people use and access technology e.g. mobile phones, games consoles, tablets and apps etc. not just laptops and computers.
- The many positive uses of technology as otherwise online safety can easily become frightening and scaremongering so be aware that the vast majority of interactions and experiences on the internet are positive!

- The importance of developing risk awareness and risk management by children and young people (according to their age and ability) and resources parents/carers can use to help discuss online safety
- Practical tips for online safety in the home such as using filters, parental controls, creating appropriate user profiles and home computer security

For further information please see: East Sussex LSCB - e-safety for parents and carers

6.4 Possible statements:

- **E** Heron Park Primary Academy recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- **E** Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
- **E** A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

Relevant for all settings

Guidance:

Schools will already have information about their obligations under Data Protection Act 1998 (the Act), and leaders should ensure that the school has a relevant policy in place. This section is a reminder that all data from which people can be identified is protected and is not a replacement for a robust data protection or data security policy.

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Act gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Act applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

If despite the security measures schools take to protect the personal information they hold, a breach of security occurs, it is important that they deal with the security breach effectively. Information security breaches can cause real harm and distress to the individuals they affect – lives may even be put at risk. Not all security breaches have such grave consequences, of course. Many cause less serious embarrassment or inconvenience to the individuals concerned. High-profile losses of large amounts of personal data have brought attention to the issue of information security; as a result the law was changed to allow the Information Commissioner (ICO) to issue fines of up to £500,000 for serious breaches of the Data Protection Act: legislation.gov.uk

For advice and guidance relating to information governance or a contravention of the Act, contact Amanda Glover: Local Authority Designated Officer, East Sussex County Council amanda.glover@eastsussex.gov.uk 01323 466606

For further information please see: East Sussex Czone School Policies - data protection

Information from the Information Commissioner's Office can be found at ICO

7.1 Statements:

- E Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- E Full information regarding the schools approach to data protection and information governance can be found in the schools information security policy.

7.2 Security and Management of Information Systems

Relevant for all settings who facilitate internet access

Guidance:

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including East Sussex Schools ICT Services.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

The East Sussex Education Network is protected by a cluster of high performance firewalls at the Internet connecting nodes in The Link Datacentres. These industry leading appliances are monitored and maintained by a specialist enterprise support team.

Schools and settings which use school provided devices which do not require pupils/staff to "login" to access systems and services (such as a bank of tablets/ iPads) must ensure there are appropriate mechanisms in place to log which member of the community has access to devices at any time to ensure that if concerns are identified, the school can trace users and take appropriate steps to ensure they are safeguarded and supported. This could include always assigning pupils/staff a specifically labelled device or routinely logging which pupil/member of staff has accessed which device.

Schools should ensure that systems and devices are suitably protected with a robust password policy. This is to protect system and network security and also prevent various concerns such as allegations against staff, data protection breaches, confidentially breaches, behaviour concerns or allegations of bullying. Passwords are a vital tool to enable school to limit access to sensitive or confidential data and

identify misuse of school systems and must not be shared or common with all but the youngest children. Members of the school community may require advice and support regarding creating safe and strong passwords.

7.2 Statements:

- E The security of the school information systems and users will be reviewed regularly.
- E Virus protection will be updated regularly.
- E Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices (*Through the Smoothwall Filtering/monitoring system)*
-

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From year *5 & 6*, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords when prompted by the school network system.

7.3 Filtering Decisions

Relevant for all settings who facilitate internet access

Guidance:

'Keeping Children Safe in Education' 2016 states that Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to online risks and should ensure that their school has appropriate filters and monitoring systems in place.

Internet access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or “allow list” restricts access to a list of approved sites. Such lists inevitably limit pupils’ access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.

The most appropriate approach will depend on the school/settings needs and requirements and will need to be considered by governing bodies and proprietors. It is recommended that governing bodies and proprietors take into account the age range of pupils, vulnerability, number of users, levels of access (e.g. how often the system is used) and the proportionality of costs vs risks when making any decisions. When reviewing filtering and monitoring systems and approach some governing bodies and proprietors may wish to undertake an approach which includes robust risk assessments and a thorough comparison which identify both the benefits and limitations of the services available to them, this may also be informed in part by the risk assessment required by the Prevent Duty.

Access profiles must be appropriate for all members of the community, for example older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily and recorded.

The UK Safer internet Centre has put together excellent guidance for schools and colleges about appropriate filtering and monitoring which can be accessed here: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring . It is recommended that governing bodies, proprietors, headteachers and DSLs read and consider this guidance when considering their own school/settings filtering and monitoring systems and any associated decisions.

Governing bodies and proprietors must make informed decisions regarding the safety and security of the internet access and equipment available in their settings. Governing bodies and proprietors must ensure that the welfare of children and young people is paramount at all times. Any decisions taken regarding filtering and monitoring systems should be taken from a safeguarding, educational and technical approach and should be justifiable and documented. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place; they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Schools and settings may also wish to approach their broadband provider to consider the range of tools available to them which may enable them to develop strategies to control and supervise their internet use and systems appropriately. Schools installing or managing their own filtering systems and policies must be aware of the responsibility and demand on management time. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the Leadership Team’s responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained and supported to be able to supervise Internet access.

Systems to enable East Sussex schools to adapt internet access according to the pupil's age, ability and maturity are available via the East Sussex Education Network. Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.

All Schools subscribing to the East Sussex Education Network receive Smoothwall web filtering as standard as a part of the package. Smoothwall meets the requirements as outlined by the Safer Internet Centre for appropriate web filtering: (saferinternet.org.uk) Filtering Monitoring Smoothwall

A common response to online safety concerns can sometimes involve schools and settings placing a reliance on technical solutions such as blocking and filtering. Whilst in some cases this may appear to be the "safest" approach, this stance does not enable or empower children to develop their own self-awareness of managing and responding to online safety risks. A more long term holistic approach should be implemented to enable children to develop appropriate skills and build resilience online according to their age, need and vulnerabilities as identified as good practice by Ofsted. This requires a coordinated approach between leaders and managers, technical, curriculum and pastoral staff.

It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules or the school Acceptable Use Policy should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and ESCC where appropriate. Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF), East Sussex Police or Child Exploitation and Online Protection Centre (CEOP) (see e-Safety contacts and references).

Websites which schools believe should be blocked centrally should be reported to the Schools ICT Service Desk. Teachers should always evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results, app etc. just before the lesson. Remember that a site or app considered to be safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page or app is accessed.

No filtering or monitoring solution can offer schools and setting 100% protection from exposure to inappropriate or illegal content, so it is equally important that they can demonstrate that they have taken all other reasonable precautions to safeguard children and staff. Such methods may include appropriate supervision, requiring children and staff to sign an Acceptable Use Policy (AUP), a robust and embedded online safety curriculum and appropriate and up-to-date staff training etc. It is vital for all Governing bodies , proprietors and members of staff to recognise that even with the most expensive and up-to-date security systems and filtering, children or staff can potentially bypass them either via using proxy sites or by using their own devices e.g. mobile phones or tablets which would not be subject to the school/colleges filtering. Appropriate supervision, policy and procedures and up-to-date education and training are essential. A reliance on filtering and monitoring alone to safeguarding children online could lead to a feeling of complacency which may put children and adults at risk of significant harm.

7.3 Possible statements:

- E The governors/proprietors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- E The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- E All monitoring of school owned/provided systems will take place to safeguard members of the community.
- E All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- E The school uses educational filtered secure broadband connectivity through the East Sussex Education Network which is appropriate to the age and requirement of our pupils.
- E The school uses Smoothwall filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, sites of an illegal nature, etc.
- E The school will work with Schools ICT to ensure that filtering policy is continually reviewed.
- E The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- E If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- E The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- E Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- E All changes to the school filtering policy will be logged and recorded.
- E The SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- E Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, East Sussex Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

Relevant for all settings who use "apps" to record children's progress

Guidance:

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at education settings which allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools will have considerable benefits for setting and their communities, including improved engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

Before purchasing or accessing any apps for staff or children's use, leaders and managers must have a clear understanding of where and how children's data will be stored within the app/tool/system, including who has access to it and any safeguarding implications. Parents/carers and staff who have access to the app must be provided with clear boundaries regarding safe and appropriate use. Schools and settings must be aware that leaders and managers are ultimately responsible for the security of any data or images held of children.

Schools and settings will need to ensure that any Acceptable Use policy (AUP) in place are up-to-date and may wish to consider implementing a specific AUP for all members of the community using the system. A specific AUP would need to include information relating to ensuring the safety of the systems including requesting that users log out of any accounts following use, use strong passwords (and requesting that users do not copy and share any images from the system. Schools and settings will need to update any parental consent forms relating to image use and data collection and may wish to amend forms to explicitly cover this use.

It also might be helpful for leaders to carry at a Privacy Impact Assessment (PIA). A PIA is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved. The ICO website has a Code of Practice on PIAs: ICO code pf practice

7.4 Statements:

- **E** The headteacher/manager is ultimately responsible for the security of any data or images held of children.
- **E** Apps/systems which store personal data will be risk assessed prior to use.
- **E** Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- **E** Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- **E** Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- **E** Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Concerns

Relevant for all settings

Guidance:

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used. An online safety policy should recognise and seek to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others.

Online Safety (e-Safety) risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Potential concerns can often be dealt with at a personal level by ensuring children are able to identify and speak with a trusted adult. Schools must ensure that all children know how to respond if they encounter unsuitable material online, for example placing a tablet screen down, closing a laptop lid, minimising a webpage or turning the screen off (not closing the page as that means the member of staff can access and report the content if required) and immediately telling a member of staff. Teachers and other members of staff are the first line of defence; their observation of classroom behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff must also be vigilant about other member of staffs' behaviour on and offline and reporting any concerns noticed should be encouraged to develop a safe culture. Incidents will vary from unintentional jokes or comments, unconsidered inappropriate action to deliberate illegal activity.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools/settings should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If schools/settings are unsure about how to respond to online safety concerns then they should consult with the SLES Safeguarding Team.

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online safety (e-Safety) incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school/setting rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Safeguarding Lead (DSL). Illegal use of internet or technology should be reported to Sussex Police.

Safeguarding concerns and incidents should be reported to Single Point of Access (SPOA), in line with East Sussex Safeguarding and Child Protection policy.

In some cases schools and settings may feel that it is necessary to contact parents/carers about an issue or alert other local school/settings. Headteachers, managers, proprietors and DSLs must ensure that they are mindful about the level of information being shared, especially if there is a live police investigation. Sharing specific information which could potentially identify children, families and schools involved or alert offenders to law enforcement investigation could result in children being placed at risk of

harm and may prevent appropriate criminal action from being taken. Ultimately this may result in a significant and long term impact on children, families and schools. Schools and settings must not release any details regarding on or offline safeguarding concerns (even if they have been shared with from a known or trusted source) which could be of detriment to any children, families or schools involved or that could jeopardise a police investigation. If schools or settings have concerns about on or offline safeguarding issues which they feel need to be shared with parents urgently, or with other schools and settings in East Sussex then they should speak with the SLES Safeguarding Team for advice and guidance.

Some schools and settings may wish to place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures.

Statements:

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
- Pupils, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the SLES Safeguarding Team or East Sussex Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to East Sussex Police.

- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the SLES Safeguarding Team.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the SLES Safeguarding Team to communicate to other schools/settings in East Sussex.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been based on content written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventually so professional judgement and support from appropriate agencies such as the SLES Safeguarding Team, Police, and Children's Social Care is encouraged.

Some settings may not feel that these sections are relevant due to the age and ability of children; however it is recommended that designated safeguarding leads ensure that their settings safeguarding policies and procedures are robust and are applicable for a range of safeguarding issues should they occur.

Some schools and settings will wish to place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures. Other settings will prefer to keep this content as reference material for DSLs.

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

Guidance:

Youth Produced Sexual Imagery or "Sexting" can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website.

Children and young people will always look to push the boundaries, especially when they go through puberty and are an age where they are more sexually and socially aware. Children typically do not use the term "sexting", usually referring to the images as "selfies" and may decide to send such pictures or videos for many reasons. For younger children (early years and primary school aged) indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour or even exploitation due to blackmail from a friend, partner, or other on or offline contact. There can also be emotional and reputation damage that can come from having intimate photos forwarded to others or shared online including isolation, bullying, low self-esteem, loss of control, creating of a negative "digital footprint" or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation.

Whilst is it important for professionals not to condone the creation of youth produced sexual imagery it is important to recognise that many young people (and indeed adults) view sharing sexual images as part of a "normal" relationship in today's modern society.

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo

images) of a person under 18 years of age, fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with consent. "Sexts" may be viewed as police evidence and it is essential that schools secure devices and seek advice immediately when dealing with concerns.

The current Association of Chief Police Officers (ACPO) position is that…. 'ACPO *does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.*'
www.ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf

It should be noted that prosecution of children for sharing indecent images for a first offence is rare. The decision to criminalise children and young people for sending sexualised images will need to be considered and made on a case by case basis based on a number of factors including age, intent and vulnerability of children involved.

'Keeping Children Safe in Education' 2016 highlights the need for all members of staff to be aware that abuse can be perpetrated by children themselves, including sexting, and there is a need for all members of staff to be aware of concerning behaviour and appropriate safeguarding responses.

It is essential that schools and settings handle 'sexting' incidents as carefully as possible and offer support to all parties involved whilst abiding by the law and also do not compromise police investigations. Should an incident arise which necessitates criminal investigation then it may require the seizure of the phone/device and any other devices involved or identified as potentially having access to the imagery. Schools and settings should ensure the existing policies regarding seizing and searching are robust and up-to-date.

Schools and education settings DSLs should access and consider the guidance as set out in UKCCIS guidance 'Sexting in schools and colleges: responding to incidents and safeguarding young people' which can be downloaded here: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Schools and settings will also want to take as many preventative measures as they can to educate young people about the risks and to support them in maintaining a healthy digital footprint. Early years and primary schools are an essential time for education regarding safe and responsible taking and sharing images as this will them to develop resilience against potential peer and social pressure to take and share sexual imagery when they are older. A range of appropriate educational resources for children and parents can be accessed in the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' document (available as above).

The statement within Appendix B may also help DSLs consider how best to respond to concerns relating to youth produced sexual imagery.

9.1 Statements:

- Heron Park Primary Academy ensure that all members of the community (of an appropriate age) are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Heron Park Primary Academy views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (*Mrs Anne Wilson*).
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- If the school are made aware of incident involving indecent images of a child the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant East Sussex Local Safeguarding Children Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The school will not view an image suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

Guidance:

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the internet. Typically this is referred to as "online grooming" however this term can sometimes be considered to be too narrow when considering online child sexual abuse as using the term "grooming" may imply that the behaviour has taken place over a period of time whilst an offender has built a relationship and gained the trust of their victim. Whilst this longer term process still occurs, current trends identified nationally (CEOP/NCA) and locally would

suggest that the period of engagement between offender and victim can in many cases be extremely brief. In 2015, CEOP identified that the objectives of online child sexual abuse have evolved and can lead to a range of offending outcomes, such as deceiving children into producing indecent images of themselves or engaging in sexual chat or sexual activity over webcam. Online child sexual abuse can also result in offline offending such as meetings between an adult and a child for sexual purposes following online engagement.

OSCE can also be perpetrated by young people themselves and these issues should be viewed and responded to in line with the East Sussex Local Safeguarding Children Board procedures.

Schools must be aware of and understand the law regarding the online sexual abuse and exploitation of children. Specifically (but not limited to):

- The Sexual Offences Act 2003 – Section 15. Meeting a child following sexual grooming.
- The Sexual Offences Act 2003 – Section 8. Causing or inciting a child under 13 to engage in sexual activity
- The Sexual Offences Act 2003 – Section 10. Causing or inciting a child to engage in sexual activity.
- The Sexual Offences Act 2003 – Section 12. Causing a child to watch a sexual act
- The Sexual Offences Act 2003 – Section 13. Child sex offences (section 10, 11 and 12) but committed by children (offender is under 18).
- The Serious Crime Act 2015 - Part 5. Protection of Children - Section 67. Sending a child sexualised communications.

More information about these offences can be found within the legal framework section of the policy template.

Schools and settings may wish to highlight responses to online child sexual abuse within existing school policies and procedures rather than within the online safety policy.

9.2. Statements:

- **E** Heron Park Primary Academy will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- **E** The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- **E** Heron Park Primary Academy views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (*Mrs Anne Wilson DHT & DSL*).
- **E** If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead should obtain advice immediately through SPOA or Sussex Police.
- **E** If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Pan Sussex Child Protection and Safeguarding Procedures

- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform East Sussex police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. or by using the Click CEOP report form: CEOP Safety Centre
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from SPOA to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

Guidance:

Schools and settings must be aware of and understand the law regarding indecent images of children. Specifically (but not limited to):

- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. The Civic Government (Scotland) Act, 1982 replicates this.
- The Sexual Offences Act 2003 (England and Wales) provides a defence for handling potentially criminal images and this is supported by a Memorandum of Understanding which provides guidance on what is and is not acceptable.

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'. More information about these offences can be found within the legal framework section.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of school computer equipment, then schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If schools are unsure if an issue is of a criminal nature then the Designated Safeguarding Lead should seek advice from SPOA or Sussex Police.

Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken. If an officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. Seizure of the server will have a significant impact on the school. It is essential that schools are aware of this possibility and they should ensure that measures are in place to enable the school's computer network to continue functioning should this situation arise.

In cases where a suspect picture or photograph is discovered it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image. There is a defence in law for police investigating crimes in these circumstances — in some cases, it may still be necessary for that person, or others (for example a person to whom an accidental find is reported), to knowingly "make" another copy of the photograph or pseudo-photograph in order that it will be reported to the authorities, and clearly it is desirable that they should be able to do so without fear of prosecution. This does not mean that schools should forward, save or print indecent images of children and as soon as schools are made aware that an image may be illegal, appropriate advice must be sough immediately. Schools should be aware that all copies (including digital or printed copies) of indecent images of children will be seized.

In all cases, a detailed statement may be obtained to assist those who investigate the offence. The following information should be included in the statement:

- The identity of any material witnesses
- The name of the Internet service provider (ISP) or mobile telephone service provider in the case of images received through a telephone
- If known, the web address, name of the app or website through which the image was found or received;
- Any passwords or other procedure required to gain access to the website
- If known, the identity of the person who sent the image
- Any details relating to those involved e.g. email address or screen names
- The reason for any delay in reporting the incident to the police (to assist investigators).

Schools and settings may wish to highlight responding to concerns regarding Indecent Images of children within existing policies and procedures rather than within the online safety policy.

9.3 Statements:

- **E** Heron Park Primary Academy will ensure that all members of the community (of an appropriate age) are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- **E** The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- **E** The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- **E** If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through SPOA and/or Sussex Police.

- If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Pan-Sussex Child Protection and Safeguarding procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), East Sussex police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via IWF .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform Sussex police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

Guidance:

Schools and settings should be mindful of the specific responsibilities and requirements place upon them under the Prevent Duty (gov.uk) Protecting Children from Radicalisation

From 1st July 2015 specified authorities, including all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015("the CTSA 2015"), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism" This duty is known as the Prevent duty. The statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

Schools are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology which includes a range of extremism views including the far right. Schools should have clear procedures in place for protecting children who are identified to be at risk of radicalisation. These procedures may be set out in existing safeguarding policies and it is not necessary for schools and colleges to have distinct policies on implementing the Prevent duty. The online safety policy will be an important part of this role as it will highlight the action that the school will take to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

'Keeping Children Safe in Education' 2016 highlights that governing bodies and proprietors should ensure that suitable filtering is in place which takes into account the needs of the schools community. Schools should ensure that online safety education highlights the risks of extremist content online, especially regarding the use and power of social media as a tool in radicalisation.

When ensuring appropriate filtering is in place, schools should be mindful to act in accordance with the law, much like when ensuring the filtering blocks other forms of illegal content. It should also be noted that radicalisation and extremist views can be shared and accessed on variety of platforms, including user generated or social media sites such as Facebook and YouTube and schools should make filtering decisions with this in mind. The way in which the monitoring of internet and network use is managed will be down to individual schools to decide and implement so as to meet their specific needs and requirements, for example taking into account the curriculum and also the needs and abilities of the community e.g. pupils or staff with English as an Additional Language. The school (Headteacher and Governing Body) needs to be able to satisfy itself that appropriate safeguarding measures (all reasonable precautions) are being taken to identify any activity which indicates that pupils or staff may be at risk of harm (or indeed putting others at risk). Leaders will need to ensure that appropriate time and resources are available to ensure that this is done sufficiently for a range of risks which will include radicalisation and extremism from a variety of perspectives as well as grooming and child sexual exploitation.

If schools/settings use devices which do not require pupils/staff to "login" to systems (such as iPads) to access the internet then they must ensure that there is appropriate mechanisms in place to log which member of the community has access to which devices to ensure that if concerns are identified, the school can trace users.

Staff with the responsibility for managing and monitoring the school filtering and network must have appropriate resources available to them as well as training and support to ensure that this can be carried out in both a manageable and a safe way. These decisions must be documented within the appropriate school policies (especially the school AUP) and be supported with training etc. and supervision all staff involved as well as the wider whole school staff and pupil group.

Schools should always be aware that simply relying on filtering to prevent radicalisation will not be sufficient as children are likely to have access to a range of devices within the home which may not be filtered or monitored, education around safe use if therefore essential. As all safeguarding risks, all members of staff should be alert to changes in children's behaviour which may indicate that they may be at risk or in need of specific help or protection. All members of staff should receive appropriate training to enable them to explore their responsibilities with regards to prevent for safeguarding pupils and adults within the school community.

School staff should also understand when it is appropriate to make a referral to the Channel programme using the Prevent Referral form (available on Czone at:
https://czone.eastsussex.gov.uk/supportingchildren/equality/Documents/Prevent School Toolkit

2015.docx). Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages.

All Prevent referrals should be made through the Single Point of Advice (SPOA)
https://new.eastsussex.gov.uk/childrenandfamilies/professional-resources/spoa/before-contact/

The Prevent team can be contacted for advice and support. Please contact Lucy Spencer, Community Safety Team

Lucy.spencer@eastsussex.gov.uk

Schools and settings may choose to highlight the overall response to the Prevent duty within existing policies and procedures rather than within the online safety policy.

Useful links regarding online hate, radicalisation and extremism

DfE: www.educateagainsthate.com
Report online hate and terrorism: www.gov.uk/report-terrorism:
NCALT e-learning http://course.ncalt.com/Channel_General_Awareness/01/index.html
National helpline: 020 7340 7264 Counter.extremism@education.gsi.gov.uk

9.4. Statements:

- E The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- E When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.
- E Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the SLES Safeguarding Team and/or East Sussex Police.

9.5. *Responding to concerns regarding cyberbullying*

Guidance:

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Cyberbullying is becoming increasingly prevalent with the rapid advances and use of modern technology. Mobile, internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide but their popularity provides increasing opportunity for misuse through 'cyberbullying', with worrying consequences. It's crucial that children and young people as well as adults, use their devices and the internet safely and positively and they are aware of the consequences of misuse. As technology develops, bullying techniques can evolve to exploit it.

When children or adults are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if those around them do not understand online bullying and its effects.

A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

Cyberbullying may not always be intentional and repeated in the same way that traditional offline bullying is. Repeated harassment online could include an initial concern which is then shared or endorsed by others such as by “liking”, “sharing” or “commenting”. People may not feel that they are bullying by doing this and single issue may become more serious. It is very important that all incidents of online abuse are addressed as early as possible to prevent escalation

Education staff, parents and young people have to be constantly vigilant and work together to prevent this and tackle it wherever it appears. Cyberbullying is a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community.

It is essential that young people, school staff and parents and carers understand how online can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school’s behaviour policy which must be communicated to all pupils, school staff and parents
- Gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where online bullying which takes place outside school is reported then it must be investigated and acted on appropriately by schools.

Under the Children Act 1989 a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm' and emotional abuse highlights the impact of online bullying. Where this is the case, the school staff should report their concerns to the SLES Safeguarding Team. Even where safeguarding is not considered to be an issue, schools may need to draw on a range of external services to support the pupil who is experiencing bullying, or to tackle any underlying issue which has contributed to a child doing the bullying.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications both on and offline could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police

For more information please read “Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies” (gov.uk) Preventing and Tackling Bullying

Childnet International have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: www.childnet.com

9.5 Statements:

- Cyberbullying, along with all other forms of bullying, of any member of Heron Park Primary Academy community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through Sussex Police.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools Online Safety (e-Safety) ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

9.6. *Responding to concerns regarding online hate*

Guidance:

Some schools and settings will prefer to integrate this content within sections 9.4 and 9.5

Schools and settings will need to be aware that whilst there is likely to be a lot of content on the internet which may be considered to be offensive, very little of it is actually illegal. UK laws have been written to ensure that people can speak and write, even offensive material, without being prosecuted for their views. However there are some situations whereby posting offensive content online may be viewed as illegal as either harassment or possibly as a hate crime. Hate crimes are any crimes that are targeted at a person because of hostility or prejudice towards that person's:

- disability
- race or ethnicity
- religion or belief
- sexual orientation
- transgender identity

Schools must ensure that they respond appropriately regarding online hate and discrimination and support members of the community who may be targeted online.

Useful links
www.report-it.org.uk – Report hate crimes
www.stoponlineabuse.org.uk - Report online Sexism, homophobia, biphobia and transphobia
www.stophateuk.org

www.victimsupport.org.uk
www.stonewall.org.uk
https://www.gov.uk/report-hate-crime

9.5 Statements:

- Online hate at Heron Park Primary Academy will not be tolerated. Further details are set out in the school policies regarding anti-bullying and positive behaviour.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Sussex Police.

Appendix B

Questions to support DSLs responding to concerns relating to youth produced sexual imagery

The following statements may DSLs to consider how best to respond to concerns relating to youth produced sexual imagery:

Child/Young person involved

- What is the age of the child(ren) involved?
    - If under 13 then a consultation/referral to Children's Social Care should be considered.
    - If an adult (over 18) is involved then police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- Is the child able to understand the implications of taking/sharing sexual imagery?
- Is the school or other agencies aware of any vulnerability for the children(s) involved? E.g. special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved? E.g. family situation, children at risk of sexual exploitation?

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats or blackmail?
    - What was the intent for taking/sharing the imagery? E.g. was it a "joke" or are the children involved in a "relationship"?
        - If so is the relationship age appropriate? For primary schools a referral to social care regarding under age sexual activity is likely to be required.
    - Is this behaviour age appropriate experimentation, natural curiosity or is it possible exploitation?
- How were the school made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another pupil or member of the school community? If so then how will the school safeguard the pupil concerned given that this is likely to be distressing to discuss.
- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?
- Is the imagery on a school device or a personal device? Is the device secured?
    - **NB: Schools and settings must NOT print/copy etc. imagery suspected to be indecent – the device should be secured until advice can be obtained**

The Imagery

- What does the school know about the imagery? (Be aware it is unlikely to be necessary for staff to view the imagery)
    - Is the imagery potentially indecent (illegal) or is it "inappropriate"?
    - Does it contain nudity or sexual acts?
- Does the child(ren) know who has accessed the imagery?
    - Was it sent to a known peer (e.g. boyfriend or girlfriend) or an unknown adult?

- How widely has the imagery been shared? E.g. just to one other child privately, shared online publically or sent to an unknown number of children/adults?

Action

- Does the child need immediate support and or protection?
    - What is the specific impact on the child?
    - What can the school put in place to support them?
- Is the imagery available online?
    - If so, have appropriate reports been made to service providers etc.?
- Are other schools/settings involved?
    - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
    - If so, what action was taken? **NB repeated issues will increase concerns for offending behaviour and vulnerability therefore an appropriate referral will be required.**
- Are the school child protection and safeguarding policies and practices being followed?
    - Is a member of the child protection team on hand and is their advice and support available?
- How will the school inform parents?
    - With older pupils it is likely that DSLs will work with the young person to support them to inform parents
- Can the school manage this issue internally or are other agencies required?
    - Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable pupils or risk of significant harm will always need involvement with other agencies.

DSLs should follow the guidance available locally by East Sussex LSCB and the SLES Safeguarding Team and nationally via "'Sexting in schools: youth produced sexual imagery and how to handle it" which can be downloaded from the UKCCIS website: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Appendix C

Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It must not replace professional advice and schools and settings should always consult with the Local Authority Designated Officer if there is a conduct issue as per the guidance and flowchart issued in July 2016. Contact should be made with the Single Point of Advice and Sussex Police if they are concerned that an offence may have been committed.

Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a "higher law" which affects all other laws. Within an education context, human rights for schools and settings to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Schools and settings are obliged to respect these rights and freedoms, balancing them against rights, duties and obligations, which may arise from other relevant legislation.

Data protection and Computer Misuse

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, video and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for

limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, organisations have to follow a number of set procedures.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

The Protection of Freedoms Act 2012

This act requires schools to seek permission from a parent / carer to use Biometric systems.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Obscene and Offensive Content, Hate and Harassment

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim’s sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

The Protection of Freedoms Act 2012 (2A and 4A) and Serious Crimes Act 2015 (section 76) - Stalking and Harassment

The Protection of Freedoms Act 2012 was updated in 2015 and two sections were added regarding online stalking and harassment, section 2A and 4A. Section 2A makes it offence for a perpetrator to pursue a course of conduct (2 or more incidents) described as "stalking behaviour" which amounts to harassment. Stalking behaviours include following, contacting/attempting to contact, publishing statements or material about the victim, monitoring the victim (including online), loitering in a public or private place, interfering with property, watching or spying. The Serious Crime Act 2015 Section 76 also created a new offence of controlling or coercive behaviour in intimate or familial relationships which will include online behaviour.

Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term "revenge porn" only applies to images or videos of those over 18. For more information access: Revenge Porn Helpline

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil "common law" tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. This act gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. The DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The School Information Regulations 2012

This act requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Sexual Offences

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

Section 15 - Meeting a child following sexual grooming. The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. This offence can result in imprisonment for up to 10 years.

Causing or inciting a child under 16 to watch or take part in a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 9. Sexual Activity with a child** (Can result in imprisonment for up to 14 years)
- **Section 10. Causing or inciting a child (13 to 16) to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 11. Engaging in sexual activity in the presence of a child** (Can result in imprisonment for up to 14 years)

- **Section 12. Causing a child to watch a sexual act** (Can result in imprisonment for up to 10 years)
- **Section 13. Child sex offences committed by children (offender is under 18)** (Can result in imprisonment for up to 5 years)

Section 16 - Abuse of position of trust: sexual activity with a child.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust and this can result in imprisonment for up to 5 years.

Indecent Images of Children

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom under two pieces of legislation; **Criminal Justice Act 1988**, section 160 and **Protection of Children Act 1978**, section 1.1.a. Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism.

A child for these purposes is considered to be anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This offence can include images taken by and distributed by the child themselves (often referred to as “Sexting”, see section 9.1). Viewing an indecent image of a child on your computer or phone means that you have made a digital image and printing/forwarding/sharing/publishing can be considered to be distribution. A person convicted of such an offence may face up to 10 years in prison.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess “extreme pornographic images”. 63 (6) identifies that such images must be considered to be “grossly offensive, disgusting or otherwise obscene”. Section 63 (7) includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.

Appendix D

Online Safety (e-Safety) Contacts and References

East Sussex Support and Guidance:

If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on:

01323 464222 or **0-19.SPOA@eastsussex.gov.uk**

If you think the child is in immediate danger, you should call the police on 999.

Sussex Police: (for non-urgent Police contact) 101 or 01273 470101

Standards and Learning Effectiveness Service (SLES): Support and Intervention Manager: Safeguarding Victoria Stutt Victoria.stutt@eastsussex.gov.uk

East Sussex Schools ICT Service: Richard May Richard.may@eastsussex.gov.uk

Local Authority Designated Officer: Amanda Glover Amanda.glover@eastsussex.gov.uk

East Sussex Safeguarding Children Board (LSCB): 01273 481544 or lscbcontact@eastsussex.gov.uk

National Links and Resources:

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Lucy Faithfull Foundation: www.lucyfaithfull.org

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/