

Heron Park Primary Academy

Acceptable Use Policy

Adopted: September 2024 Review date: September 2025

This policy outlines what are acceptable and unacceptable uses of ICT facilities within Heron Park Primary Academy. It is relevant to pupils, staff, LAB members and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies, we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

At Heron Park Primary Academy, we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet.
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner, which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognise that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Headteacher or her/his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems
- Reporting any inappropriate behaviour and online bullying to the E-safety Coordinator
- Take reasonable care that there is no damage or loss of any equipment on loan from school

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or non-productive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or taking photographs on school premises without permission and with consent of the parent or carer.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list, unless something being sent to the whole school for information.
- Relocating school information and communication equipment without prior permission
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers
- Doing harm to other people or their work.
- Do not install software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper-case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the school's address instead, but not the school's phone number.
- Downloading material from the Internet without specific authorisation from the ICT manager.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.

I understand these guidelines and agree to follow them.

Full name		Role	
Signature		Date	