Kingswood House School
IT Acceptable Use Policy

Created by **Sally Witts**
Updated by **Pippa Webb 14 July 2022**
Review date **July 2023**

Interaction with other policies

There is a clear overlap in this area between staff and pupil conduct, data security, child protection, personal privacy online, and good practice including around digital record keeping (including both email use and retention). This means that the Acceptable Use Policy does not stand on its own but must sit alongside related policies (applicable to staff or pupils), including where applicable:

(a) Privacy Notices (those aimed at pupils / parent and staff);
(b) Child Protection and Safeguarding Policy;
(c) Staff Code of Conduct;
(d) Data Protection Policy;
(e) Anti-Bullying Policy;
(f) Whistleblowing Policy;
(g) E-Safety Policy;
(h) Taking, Storing and Using Images of Children Policy;
(i) Storage and Retention of Records and Documents Policy;
(j) Policy on Pupils' Use of IT, Mobile Phones and Other Electronic Equipment:
(k) Bring Your Own Device (BYOD) Policy.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers. It applies to the use of computers, laptops, mobile phones, tablets, digital cameras and any other electronic devices. The advice given also applies to their use outside school since our aim is to teach pupils to use technology safely at all times.

Online behaviour

The following paragraphs refer to the use of all electronic devices, whether purchased via the school or brought in.

Adhere to the same standards of behaviour online that you follow offline. Be polite. Abusive, derogatory language or cyber-bullying is not permitted or tolerated.

The school will adopt a **zero tolerance approach** to any cyber bullying issues and all staff will challenge any abusive behaviour between peers that comes to their notice and will report on to the DSL immediately any issues of this nature.

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Pupils and parents will be asked to sign an agreement for responsible computer and internet use. See Appendix 1.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- External hard drives and USBs are not permitted in school.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Bursar.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Chromebooks and iPads

Pupils with Chromebooks or iPads must adhere to the following:

- Pupils must bring their laptops to all classes, unless a teacher specifies otherwise. It is the pupil's responsibility to ensure that their laptop is fully functional at all times, and if not to report the problem to the ICT department at their earliest opportunity.
- When a device is not in the pupil's possession, it must be locked in a designated secure location and never be left unattended in any part of the site.
- iPads and Chromebooks must be kept in the approved case/sleeve at all times and clearly named. Name labels must not be removed.
- Only the supplied power adaptor may be used with school scheme devices. Replacement chargers may only be purchased via the school.
- Devices are to be charged at home to avoid the disruption caused to lessons of laptops running out of battery power.
- Damaged or faulty devices or chargers must be reported to the ICT department immediately and not used as they could be potentially hazardous.

Device identification

It is statutory that each laptop and case exhibit the pupil's name clearly. Luggage tags and paint pens are recommended. Personal laptops brought independently of the school's laptop scheme are the responsibility of the owner.

Procedure if a Chromebook or iPad is missing

If a device cannot be found whilst in school, the pupil must report the matter to a member of staff and the ICT department. If the laptop goes missing from outside the school premises or theft is suspected the parents of the pupil must report this theft to the police immediately. The suspected theft or loss must then be reported to the ICT department.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered with and approved by the Senior Leadership Team. Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies.

Monitoring and access

Staff, parents and pupils should be aware that school computer systems (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others. Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be routinely kept in archive whether or not deleted and email accounts will be closed and the contents deleted / archived within 1 year of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Bursar.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the Information Commissioners Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they must contact a member of the Senior Leadership Team or Headmaster immediately.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to a member of the Senior Leadership Team. Reports will be treated in confidence.

Recording of internet safety incidents

The school maintains records of all internet safety incidents. Any such incident is reported to the Designated Safeguarding Lead. Offsite instances using other technologies are more difficult to track, but without going beyond its legal parameters, the school will act upon all information provided where appropriate.

CCTV

Kingswood House School believes that closed circuit television cameras (CCTV) offers improved security protection for both pupils and staff. The School has CCTV installed on its premises for the sole purpose of surveillance for security reasons. Notices are clearly displayed in areas around the school. It is not installed in classrooms, changing rooms or toilets.

Kingswood House School is registered with the Information Commissioner's Office and has an appointed member of the school's management team who oversees all aspects of the use of surveillance CCTV within the school. Parents are assured that the School does not stream images collected via CCTV to any third parties or outside agencies. Please note that the school may be legally required to provide CCTV footage to the police

Appendix 1

PUPIL AGREEMENT

Rules for Responsible Computer and Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- I will only access the system when a member of staff is present in the room and I have permission.
- I will not access other people's files without permission.
- I will only use the computers for school activities.
- I will not bring in USBs, DVDs or CDs from outside school unless I have been given permission from the ICT department.
- I will only e-mail people I know, and whom my teacher has approved, and only when my teacher gives me permission.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone by email, unless my parent, carer or teacher has given permission.
- I will report any unpleasant material or messages sent to me in order to protect other pupils and myself.
- I will only access websites that I am directed to by my teacher.
- I will only print with the permission of my teacher.

Pupil's Signature…..……..... Date……...…….

Parent's Signature…… Date…….