Derby
Grammar
School

Bringing education to life.

IT Acceptable Use Policy

Scope:	Whole School including EYFS
Release date:	September 2023
Review date:	September 2024
Author:	Assistant Head Pastoral
Reviewer:	Head and Governors

Linked Documents

7h E-safety and Filtering Policy

Availability

This policy is available on the School website or may be requested from the School office. Any printed or local copies must be checked against the website version to ensure they are current.

Acronyms

IT	Information Technology
ICO	Information Commissioner’s Office
CPO	Chief Privacy Officer

This policy applies to all members of the school community, including staff, pupils, parents, contractors, third parties 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.

Online Behaviour

As a member of the school community you must 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 capture or share photos, videos, audio recordings, 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 must not use their personal email, or social media accounts to contact pupils or parents, and pupils and
- Parents must not attempt to discover or contact the personal email addresses or social media accounts of staff.
- Be aware that “upskirting” (the practice of taking unauthorised photographs under a woman's skirt or man's kilt, capturing an image of the crotch area, underwear, and sometimes genitalia.) became a criminal offence in April 2019. An “upskirt” is a photograph, video, or illustration which incorporates an image made by “upskirting”.

Using the school's IT systems

Whenever you use the school's IT systems, where permitted (including by connecting your own device to the network), you must 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.

● The school monitors use of the school's IT systems, and can view content accessed or sent via its systems.

Passwords

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

Passwords must contain 8 characters or more and be any combination of letters, numbers and symbols. Passwords to the G-suite and network will be reset automatically ready for the start of the academic year.

All users will be prompted to renew their password for G-suite access at regular intervals.

Use of property

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

Use of school systems

The provision of school email accounts, Wifi and internet access is for official school business, administration and education. Staff and pupils must keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of school accounts. Please be aware that the school monitors email and internet use and when required will review the use of these facilities in the event of an investigation or notification of inappropriate/unauthorised use.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, using school provided user accounts, 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 or cloud storage must be registered and approved by the School.

Where permission is given for the use of personal devices, these must be subject to appropriate safeguards in line with the school's policies. Please seek advice where necessary.

In certain circumstances pupils may be allowed to use their personal devices, laptops, mobile phones, in a classroom setting. Personal devices must only be used with the permission of the member of staff.

Monitoring and access

Staff, parents and pupils must be aware that school email and internet usage (including through school Wifi) 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. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies

You will ensure that you comply with the school's Privacy Notice and relevant policies, e.g. Data Retention, Taking and Using Images, Safeguarding and Anti Bullying.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted and email accounts will be closed and the contents archived within one year of that person leaving the school. Important information that is necessary to be kept must 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. That way no important information should ever be lost as a result of the school's email deletion protocol.

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 School Business Manager.

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, password breach or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post or email;
- failing to bcc recipients of a mass email;
- unsecure disposal.

The school must generally report personal data breaches to the 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, please make contact with the Chief Privacy Officer (CPO) 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 which could result in a fine from the ICO.

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 or withdrawing 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 must report it to the Designated Safeguarding Lead. Reports will be treated in confidence.

Please click here to digitally sign this policy.