IT Acceptable Use 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.

Online behaviour

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.

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.

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

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.

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 (i.e. school email accounts on mobile phone / tablet) 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 and approved by the Head.

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

Taking Documents Home: Securing Personal Data

Under the GDPR staff should do everything in their power to prevent a breach of personal data. This includes ensuring that any physical documents containing personal data taken home by staff are kept secure, to prevent the data from being lost, stolen or accidentally leaked.

Staff should only access pupil personal data via ISAMS remotely, data stored in ISAMS is secure and cannot be misplaced or lost.

Documents such as exercise books or coursework contain little personal data and may be taken home by staff for marking, however, documents with more substantial amounts of personal data for example; pupil records, annual or termly reports and pupil references need to be handled in a more secure manner and should not be removed from the school. Reports written in ISAMS, CPOMS or Tapestry are secure, reports written in Word should be treated as personal data and every effort must be made to ensure that these are kept secure.

Individuals also have legal rights to:

• require us to correct the personal data we hold about them if it is inaccurate;

• request that we erase their personal data (in certain circumstances);

• request that we restrict our data processing activities (in certain circumstances);

• receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;

• object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

• object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell Lisa Maynard, Director of Operations as soon as possible.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (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. 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.

Pupil files held in the school office when removed must be signed out by staff and signed in on their return. These documents contain personal data and must not be left unattended and should be locked away when not in use.

Documents containing pupil details taken off site i.e during PE or on a trip should be secured in a file with a zip lock, clearly labelled with the school's or member of staff's name and address to enable return. These documents should also be signed in and out of the office and must be kept secure whilst off site.

Any breach should be reported to the Director of Operations immediately.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy, Retention of Records, Safeguarding, Anti-Bullying and Acceptable Use Policy.

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 deleted 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. 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 Head.

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 Commissioner's Office (ICO) without undue delay (ie 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, you should notify the Director of Operations (Schools) 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 the Director of Operations (Schools). Reports will be treated in confidence.