7g. Acceptable Use of IT 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, if applicable, 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 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, 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 personal social media accounts to contact pupils or parents. 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.
- Pupils are responsible for using the school IT systems in accordance with the E-safety Policy and for letting staff know if they see IT systems being misused. If pupils are accessing their email accounts (both e.lyceum and lyceum.co.uk), this should only be used for school related tasks such as projects and homework.

Passwords

Passwords protect The Lyceum's network and computer system 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. You must change your password 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. Please be aware of the school's right to monitor and access web history and email use.

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 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 E-safety, Safeguarding, Anti-Bullying and Acceptable Use of IT Policies.

Retention of Digital Data

Staff and pupils must be aware that all emails sent or received on school systems may be kept in archive even if deleted. 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. However, the work of pupils is cloud based through Google Classroom and Google Drive; this is monitored by Compatibility through Google Workspace and Google Admin.

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
- 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 Head of Operations and Compliance 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 if you are concerned that a member of the school community is being harassed or harmed online, you should report it to a member of SLT or to the Safeguarding Governor for The Lyceum. Reports will be treated in confidence.