Acceptable Use of Technologies Policy

Review Date: May 2023
Review by: Personnel/Student Care and Discipline
Final Approval by: Personnel/Student Care and Discipline

Academy Context

The Core Values of the academy which relate specifically to this policy state that we are working together to form relationships based on

- **Justice** – everyone in academy is entitled to be treated fairly and to promote the self-esteem of others.
- **Responsibility** – everyone in academy is expected to understand the consequences of their actions.
- **Truth** – everyone in academy is required to be honest and to communicate in a positive manner.

Such values contribute to our common purpose of "Striving for high quality education with a strong Christian ethos", and as such underpin procedures within the Academy.

Data Protection

Any personal data processed in the delivery of this policy will be processed in accordance with the academy Data Protection policy.

Introduction

- Digital technologies have become integral to all of our lives. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Users have an entitlement to safe internet access at all times.
- This Policy is intended to ensure that users will be responsible and stay safe while using the internet and other digital technologies for educational use, and that academy systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- The academy will provide good access to digital technologies to enhance their learning and will, in return, expect all users to be responsible.
- Use of the Internet and any other technologies on academy equipment, both in the academy and outside, can be monitored and logged by the IT team and academy leaders.
- While it is not possible to cover every possible scenario, general principles of common sense, lawful activity and safeguarding will guide all responses to misuse.
- This Policy should be read in conjunction with the Safeguarding suite of policies, *Keeping Children Safe in Education* (2020), Behaviour Policy (students) and the Disciplinary Policy (staff), the GDPR and academy GDPR policies.

Acceptable Use

Acceptable use includes:

- Ensuring online activity, both in academy and outside academy, will not cause academy users or others distress, or bring the academy into disrepute.
- Protecting users from all messages of violent extremism online or using any means or medium to express views that
  - ❖ encourage, justify or glorify political, religious, sexist or racist violence
  - ❖ subscribe to rigid and narrow ideologies which are intolerant of diversity, leaving those who hold them vulnerable to future radicalisation
  - ❖ foster hatred which might lead to inter-community violence in the UK
  - ❖ seek to provoke others to terrorist acts
  - ❖ encourage other serious criminal activity or seek to provoke others to serious criminal acts

- Respecting copyright and the privacy and ownership of other people's work and acknowledging the source of information used.
- Questioning the reliability of material published on the Internet.
- Understanding that the Acceptable Use Policy is designed to keep users safe. If not followed, academy sanctions will be applied.
- Not deliberately browsing, downloading, uploading or forwarding material that could be considered offensive or illegal. If users accidentally come across any such material they should report it immediately.
- Not giving out own or others' personal data such as name, phone number, address, passwords.
- Not arranging to meet someone unless this is part of an academy project approved by a teacher.
- Reporting incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies.
- Not taking or using images of users, except in line with their data consent, and storing and using those only for purposes for which consent has been given.
- Not uploading or add any images, video, sound or text which could upset or offend another person.
- Not attempting to bypass the internet filtering system.
- Not using proxy sites.
- Not using chatrooms, gaming or social network sites in the academy.
  Participating in line with academy guidance when taking part in remote learning
  Never recording a remote learning session, or screen shotting any part of an online learning session.

Acceptable use of Academy Equipment
Users are expected to use hardware (eg computers, printers) within academy or other settings in an appropriate manner. This includes:

- Only using ICT systems in academy, including the Internet, Firefly, email, digital video, mobile technologies, etc. for academy purposes.
- Logging on to the academy network/ VLE (Firefly) and other packages from the academy using own user name and password.
- Not revealing passwords to anyone and changing passwords regularly.
- Staff must change their passwords every twelve months.
- Only opening and / or deleting own files.
- Only printing text and images which are required for educational purposes.
- Ensuring memory sticks or other transferable data files have been virus checked to minimise issues of virus transfer.
- Do not leave your PC or laptop unlocked. Ensure that you lock your PC before leaving your desk.
- Not downloading or installing software onto academy technologies.

(Any proposed installation of software onto staff laptops/PCs should be checked with the ICT department first. It reserves the right to remove any software which has not been authorised by them or is deemed to be a risk to the academy's network.)

Appropriate use of e-mail
The use of e-mail within the academy is an essential means of communication. All users are given their own e-mail account to use for all academy business. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. However wherever academy e-mail is accessed (whether directly, through webmail when away from the office or on non-academy hardware), the acceptable use policy applies.

Acceptable use of e-mail includes:

- Keeping email passwords secure.

- Ensuring that all ICT communications with users or others is responsible and sensible.
- Using language which is appropriate.
- Not sending file or image attachments which would cause offence.
- Not sending emails to large groups without prior permission.
- Not forwarding chain letters/ emails using academy email.
- Not revealing any personal data about self or others.
- Immediately reporting the receipt of any offensive e-mail.
- Never knowingly opening attachments from an untrusted source.

Appropriate use of the Virtual Learning Environment (VLE) (Firefly and Shared Areas)
The VLE provides a wealth of opportunity within and beyond the academy to access resources, collaborate and share work. Appropriate use of the VLE includes:

- Not uploading files or images which could cause offence.
- Not uploading any material which is confidential or copyrighted unless permission has been obtained.
- Not using the VLE in such a way that it disrupts the use of the VLE by others.
- Not using other users' passwords or allowing others to use a personal password.
- Not uploading or using malicious code in any form.

Acceptable use of Mobile Devices and Other Technologies
When mobile phones or smart watches are used in the Academy by students, they will be confiscated and kept by Student Services for the rest of the day.

Acceptable use of:
(i) Personal mobile devices

- Access can be made to academy email on mobile devices such as private laptops, iPads and smartphones but such devices must be encrypted. Encryption will be enforced via password protection in the first instance. Any device that has access to academy's email system without a password will be denied, until such time that device meets requirement set out in this policy.
- Users can access the academy's wireless network by entering username and password.
- Users must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- The academy is not responsible for any theft, loss or damage of any personal mobile device.
- Mobile devices (both academy issued and personal) which have academy email accounts set up on apps will be erased in the event of loss or theft in order to avoid access to personal data in line with Data Protection legislation.

(ii) Academy mobile devices

- Where the academy has provided a mobile device, such as a laptop, iPad or mobile phone, this equipment should only be used to conduct academy business in any location.
- Equipment provided by the academy should not be used to store large quantities of personal files.
- Any personal files stored on mobile devices must comply with the provisions of the Data Protection legislation.
- Mobile devices should only be used to connect to a digital projector or Apple TV under authorised circumstances.
- Professional documents which contain academy-related sensitive or personal data (such as children's reports and data, including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones) must be protected by encryption. Any devices which provide access to professional documents must be protected from

unapproved access or theft. Encryption must be used when transferring any personalised documents onto portable devices. (e.g USB pen drives, external hard-drives)

Acceptable use of Images

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. The academy has the following devices available:

- Digital cameras
- Video cameras
- Web cams
- Drone cameras

In all possible situations, academy issued equipment must be used. If personal equipment is used permission must be granted by a teacher.

- Personal images must not be uploaded onto personal space (My Documents/ OneDrive) or on to the Virtual Learning Environment (VLE), without express permission.
- It is recommended that permission is sought prior to any uploading of images to check for inappropriate content.
- Uploaded images must not have a file name of a person.
- Images must not be of any indiscrete nature (eg people in compromising positions or in inappropriate clothing).
- Any images taken and used by the academy on the website or for other purposes will be in accordance with the procedures issued in the induction packs.
- The sharing of images via weblogs, forums or any other means on-line will only occur after consent has been given by the user in line with the GDPR.