Acceptable Use Policy

Review Date: May 2020

Review by: Personnel/Student Care and Discipline

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

- **Justice** – everyone in school is entitled to be treated fairly and to promote the self-esteem of others.
- **Responsibility** – everyone in school is expected to understand the consequences of their actions.
- **Truth** – everyone in school 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 School.

Data Protection

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

Acceptable use of the Internet

Acceptable use of the internet includes:

- Ensuring online activity, both in school and outside school, will not cause the school, the staff, students or others distress or bring the school into disrepute.
- Protecting students against all messages of violent extremism 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 that are intolerant of diversity, leaving those who hold them vulnerable to future radicalization
  - ❖ 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 students safe and that if not followed, school sanctions will be applied and parents may be contacted.
- Not deliberately browsing, downloading, uploading or forwarding material that could be considered offensive or illegal. If students accidentally come across any such material they should report it immediately.
- Not giving out any personal information such as name, phone number or address.
- Not arranging to meet someone unless this is part of a school project approved by a teacher.
- Reporting incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies.
- Images of students and staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission.
- Not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- Not attempting to bypass the internet filtering system.
- Not using proxy sites.

- Not using chatrooms or social network sites in school.
- Understanding that use of the Internet and other related technologies can be monitored and logged and can be made available to the e-safety leader

Acceptable use of School Equipment
Users are expected to use computers, printers and other technologies within school or other settings in an appropriate manner. This includes:

- Only using ICT systems in school, including the Internet, Firefly, email, digital video, mobile technologies, etc. for school purposes.
- Students and teachers logging on to the school network/ VLE (Firefly) using own user name and password.
- Not revealing passwords to anyone and changing them every six months.
- Only opening and / or deleting your own files.
- Only printing suitable 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.
- Not downloading or installing software onto school technologies.

Appropriate use of e-mail
The use of e-mail within the school is an essential means of communication. The school gives all users their own e-mail accounts to use for all school business as a work based tool. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. However school e-mail is accessed (whether directly, through webmail when away from the office or on non-school hardware) all school e-mail policies apply.

Acceptable use of e-mail includes:

- Keeping email passwords secure.
- Ensuring that all ICT communications with students, teachers 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 of students without prior permission.
- Not forwarding chain letters/ emails using school email.
- Not revealing any personal details about self or others.
- Immediately reporting the receipt of any offensive e-mail.
- Never opening attachments from an untrusted source.

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

- Not uploading files or images that 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 are used in unauthorised circumstances they may be confiscated and kept by Student Services for the rest of the day.

Please refer to the Personal Electrical & Electronic Equipment Use Policy for details on the charging of mobile devices in school.

Acceptable use of:

(i) Personal mobile devices

- Access can be made to school email on mobile devices such as PDAs 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 School'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 school's wireless network by entering their 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 school is not responsible for any theft, loss or damage of any personal mobile device.
- Mobile devices (both school issued and personal) which have school 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) School issued mobile devices

- Where the school has provided a mobile device, such as a laptop, iPad or mobile phone, this equipment should only be used primarily to conduct school business both inside and outside the school environment.
- Equipment provided by the school 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 school-related sensitive or personal information (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 video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access if required for students to use:

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

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

- Personal images should not be uploaded onto personal space (My Documents) 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 should not have a file name of a student, especially where these may be uploaded to a school website.
- Images should not be of any compromising positions or in inappropriate clothing.
- Any photographs taken and used by the school on the website or for other purposes will be in accordance with the photograph procedures issued in the induction packs.
- The sharing of images via weblogs, forums or any other means on-line will only occur after permission has student been given by the parent