St Wilfrid's
Church of England Academy

E-Safety Policy

Non Statutory Policy

Created by: Mr N Ashman

Date presented to governors: 24 March 2022
Review Date: Spring 2024
For public internal viewing

Link to other policies:

- Social Media Policy
- iPad Acceptable use Policy
- Behaviour for Learning Policy
- Mobile Phone Policy
- Data Protection Policy
- Privacy Policies
- Staff Discipline Policy
- Allegations and concerns raised in relation to staff, supply staff, contractors and volunteers Policy

St. Wilfrid's C of E Academy
E-Safety Policy

Contents

1. Rationale

The use of 'Information and Communication Technologies (ICT) has great benefits for the development of students' learning and the administration and governance of an Academy. With these advantages, however, come significant risks, including:

- Sexual exploitation;
- Identity theft;
- Spam;
- 'Cyber' bullying;
- Viruses;
- Grooming;
- Access to inappropriate content.

2. Policy aims

It is the aim of this policy to minimise these risks for:

- Students;
- Staff and others involved with the daily activities of the Academy.

This policy, supported by the Academy's acceptable use agreements for staff and students (Appendix 1), is to protect the interests and safety of the whole academy community. It is linked to the following mandatory academy policies: child protection, health and safety, and behaviour/student discipline (including the anti-bullying) policy and PSHE.

3. What is 'Un-safe' use of ICT

This policy is concerned with significantly unsafe use of ICT, not minor infringements. Just as safe use of ICT is commonly known as e-safety, unsafe use of ICT is an e-safety incident. E-safety incidents:

- Use some form of technology;
- Causes or could have caused significant offence, harm or distress;
- May or may not be deliberate;
- May not have occurred within academy or on academy equipment.

Examples of e-safety incidents (not exclusive) include:

- A student or member of staff viewing inappropriate material on an academy computer such as pornography, weapons, banned substances or any age restricted material;
- A student bullying someone from another school with text messages, group chat messages or videos on video sharing sites;
- A student bullying a fellow student using instant messaging services such as WhatsApp, Snapchat or Instagram from home;
- A student placing distressing posts about a member of the Academy community on social networking sites like Facebook or Instagram;
- A student publishing their own personal details such as their address on the internet;
- A student publishing revealing images of her or himself on a social networking site or within a message on apps such as Snapchat or WhatsApp;
- A student sharing a video taken on a mobile device of a member of staff in a lesson with other students;
- A member of staff suspecting a student of being groomed;
- A student modifying a photo of a member of staff and distributing it physically or on the internet;

- A student taking a picture or video on school premises and sharing it physically or posting it online via social media or through a messaging app.

4. Staff Responsibilities

4.1. E-Safety Coordinator

Each Key stage has an 'e-Safety' Coordinator. These are; KS5, Assistant Principal – Sixth Form, KS4, Assistant Principal - KS4, KS3, Assistant Principal – KS3, with the designated Child Protection officer Vice Principal – Safeguarding overseeing cases ; all members of the academy community will be made aware of who holds this post. These individuals will take advice from Lead Teacher New Technologies and the Network Services Manager where it is deemed appropriate.

It is the role of the e-Safety Coordinator to:

- Keep abreast of current issues and guidance through organisations such as BwD, CEOP (Child Exploitation and Online Protection) and Childnet;
- Support staff in handling incidents;
- Support education of students and staff in the safe use of ICT.

4.2. Network services manager

It is the role of the Network services manager to maintain services in support of the safe use of ICT.

Typically to include:

- Internet and email filtering and logging;
- Classroom management tools to monitor ICT use;
- Network access logging;
- Appropriate level of network security against malicious use.

4.3. Other Staff

Staff within the Academy must:

- Know what is safe use of ICT;
- Model safe use of ICT within the academy community and beyond;
- Be alert to unsafe use of ICT, by students & staff within the academy and beyond;
- Manage & report incidents as appropriate;
- Educate students where required by the curriculum.

5. Student Responsibilities

Every student must:

- Adhere to the Acceptable Use Policy (See Annex 1)
- Report incidents as they occur through the most appropriate member of staff; current teacher, form tutor or e-Safety Coordinator

6. Parent Responsibilities

Every Parent / Carer must:

- Understand the Acceptable Use Policy and encourage their child to use ICT safely;
- Accept any sanctions that are applied when a student breaches the policy.

7. Education in safe use of ICT

7.1. Staff

- All staff will be trained in the safe use of ICT both for themselves and for students they supervise.
- This will be incorporated with the 2 year refresher training in Child Protection.
- New staff will receive information on the Academy's Acceptable Use Policy as part of their induction.
- The training will raise awareness of their individual responsibilities for the safeguarding of children within the context of e-Safety and will cover what to do in the event of misuse of technology by any member of the academy community.

7.2. Students

- The Academy will provide opportunities through the main areas of ICT, PSHE and through Assemblies and supported in other curriculum areas as appropriate and other more informal settings e.g. Form time.
- Year 7 students will cover E-safety topics during their two-day iPad induction.
- The ICT curriculum will include relevant legislation such as Data Protection and intellectual property laws which may limit what they want to do but also serves to protect them.
- Students will be taught about copyright and respecting other people's information, images, and related topics.
- Students will be made aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be taught the dangers of releasing personal information through the use of social networking platforms and instant messaging / chat facilities. Where these technologies have good educational outcomes they will be available within our network services.
- Students will also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. SHARP online system parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

8. Managing Technology

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internal use of the Academy's network is logged to allow any inappropriate use to be identified and followed up.

8.1. Infrastructure

Staff will monitor access and use of the Academy network including internet services, so activity is checked and recorded. Email and internet activity can be monitored and explored further if required.

St Wilfrid's will be aware of its responsibility when monitoring staff and student communication under current legislation and take into account:

- Data Protection Act 1998;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- Regulation of Investigatory Powers Act 2000;
- Human Rights Act 1998;
- General Data Protection Regulation 2018.

The Academy will use management control tools for controlling and monitoring workstations.

8.2. Managing the Internet

- All access to the internet will be monitored. This includes mobile devices managed by the Academy.
- Staff will make every effort to preview sites before recommending them to students; it is recognised that internet sites are beyond the control of the Academy.
- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or illegal software from other sources.
- All users should make all reasonable attempts to observe copyright of materials from electronic resources.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Users must not reveal personal information about members of the academy community (including names) acquired through academy life on any social networking site or blog without seeking the subject's permission. Information published on the internet prior to the adoption of this policy may remain where it does not cause an issue, however staff should declare any new material in the public domain to the Principal which will be inspected for suitability.
- Collaborative learning or blogging activity must be carried out only on the Academy managed service e.g. an internal server or hosted solution.

9. Communication

Students, Parents, Staff and Governors are made aware of the Academy's e-Safety Policy through a variety of means:

- The e-Safety policy will be introduced to the students at the start of each academy year through the ICT and Personal Development Curriculum;
- e-Safety messages will be embedded across the curriculum whenever the internet and/or related technologies are used including Assemblies and Guidance sessions;
- e-safety posters will be prominently displayed.

E Safety updates will be displayed by the following methods-

- Academy Website;
- Firefly;
- Academy Screen Savers;
- Information monitors/ Screens around the Academy.

10. Specific E-safety issues

Further advice available http://www.itgovernance.co.uk/

11. Digital images and video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the academy community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of students) and staff, the academy permits the appropriate taking of images by staff and students. Staff should only take photographs or videos of students with the express permission of student and parent. This is normally obtained from parents on

entry to the academy and a list of the students whose parents have objected to this is kept by the Data Manager. It is preferred that the academy equipment is used for this, but in any case, images must be transferred within a reasonable time scale and solely to the academy's network or hosted services controlled by the academy and deleted from the original device.

Students must be advised when using their personal digital equipment, especially during field trips, that images and video should only be taken with the subjects' consent. Students should also be advised that complaints against this condition will be considered a serious breach of this policy and risk having the device confiscated until it can be inspected, in their presence, by the e-safety co-ordinator or a member of the Senior Leadership Team.

Permission to use images and video of all staff who work at the Academy is sought on induction and a copy is to be stored in the relevant personnel file.

Publishing Student's Images and Work
On a student's entry to the academy, all Parents/carers are asked to give permission to use their student's work / photos in the following ways:

- On the academy website;
- On the academy's Learning Platform;
- In the academy prospectus and other printed publications that the academy may produce for promotional purposes;
- Recorded/ transmitted on a video or webcam in display material that may be used in the academy's communal areas;
- In display material that may be used in external areas, i.e. exhibition promoting the academy general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by all interested parties in order for it to be deemed valid. Students' full names will not be published alongside their image by the academy and vice versa. E-mail and postal addresses of students will not be published. Often, the press wishes to publish full names for members of teams. In these cases, the member of staff supervising will ensure that appropriate permission is sought. Before posting student work on the Internet, the member of staff responsible must check that permission has been given for work to be displayed.

Video Conferencing (includes Teams, Zoom and Face Time)

- All students are supervised by a member of staff when video conferencing.
- Any conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference with end-points outside of the Academy is to be recorded in any medium without the written consent of those taking part.
- Remote learning will take place via Microsoft Teams only, where only participants with a saintwilfrids.com email address can attend. Teachers and students must then adhere to remote learning guidance given on the Firefly learning platform.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

For further information and guidance relating to Video Conferencing, please see:
http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

12. Personal Mobile Devices (PMDs) including iPads, phones and other PMDs provided by the Academy

The Academy allows staff to bring in PMDs for their own use. Under no circumstances does the Academy allow a member of staff to use their personal mobile phone to contact a student. Staff are advised not to contact a Parent / Carer using their personal mobile phone but there may be circumstances concerning a duty of care to students which override this. In these cases staff are advised to block their number, prior to making the call.

Students are allowed to bring PMDs into the Academy – use of these is covered by our Acceptable Use of iPad Policy (Annex 1) and Mobile Phone Policy.

The Academy is not responsible for the loss, damage or theft of any personal PMD.

The sending of inappropriate (as determined by any involved party) text messages between any member of the Academy community is not allowed.

Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community.

Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

Where the Academy provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, these devices must be used rather than a personal device.

Staff must use password protection for their PMD in case of theft, and any staff losing a PMD which is configured for Academy data services must report the loss to the academy as soon as practical. The Academy will then prevent further access by the device.

13. Further Guidance

Websites offering help and advice:

- http://www.anti-bullyingalliance.org.uk
- http://www.itgovernance.co.uk/
- http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml
- http://www.thinkuknow.co.uk
- http://www.leedslearning.net/documents/e-safety/Chat%20Room%20Dangers%20and%20computer%20safety.doc
- http://www.ceop.gov.uk/

- http://www.getsafeonline.org/
- http://www.parentscentre.gov.uk/flash/safety/main.swf
- http://www.kidsmart.org.uk/
- http://www.microsoft.com/athome/security/children/default.mspx
- http://www.parentscentre.gov.uk/
- http://schools.becta.org.uk/index.php?section=is
- http://publications.becta.org.uk/display.cfm?resID=32424&page=1835
- http://www.digizen.co.uk/
- http://www.portal.northerngrid.org/ngflportal/custom/resources_ftp/client_ftp/ e-Safety_audit_tool/e-Safety_audit_tool.html
- http://www.nextgenerationlearning.org.uk/safeguarding

14.Procedures for handling and reporting Incidents

Student e-safety incidents

Many incidents of misbehaviour involving ICT do not lead to actual or potential significant offence, harm or distress. These should be dealt with by our normal discipline procedures. Where the member of staff involved believes the event to be an e-safety incident, they will follow this procedure:

- Log the incident via email to the relevant Keys Stage e safety coordinator. This should be seen as a neutral act to protect all parties;
- If the incident constitutes misbehaviour the member of staff must add a behaviour comment onto the SIMS system;
- The appropriate e-safety co-ordinator will investigate and decide if further action is necessary;
- Further action may include sanctions or education and may involve parents. In extreme cases, it may be necessary to involve outside agencies such as the Police;
- The e-safety co-ordinator will inform pastoral staff as appropriate and report the outcome of any investigation to the member of staff who reported the initial incident.

Staff e-safety incidents

If a member of staff suspects another member of staff has breached this policy, they should report their concerns to Principal. The Principal will investigate to see if further action is needed and report to the relevant authorities. Any internal disciplinary action taken will conform to the Staff Discipline policy. If a criminal offence has been committed, the details will be passed on to the appropriate agencies.

Appendix 1

iPad/ Acceptable Use Policy for Students

The policies, procedures and information within this document apply to all iPads/ Mobile devices used by students in the Academy.

General Care and Guidance

iPad batteries need to be charged and be ready to use in the academy.

Syncing the iPad to iTunes or iCloud will be the student's responsibility.

Items deleted from the iPad cannot be recovered.

Memory space is limited. Academic content takes priority over personal files and apps.

The whereabouts of the iPad should be known at all times.

It is students' responsibility to keep their iPad safe and secure.

iPads belonging to other Students are not to be meddled with in any way.

If an iPad is found, it should be given to an IT Technician within the LRC

Students must use covers or cases that protect their iPad.

Only a soft cloth, or laptop screen cleaning solution from the Academy's IT technicians is to be used to clean the iPad screen.

Do not let the iPad get very hot or cold.

Do not leave the iPad in the academy overnight or in vehicles.

Students may not photograph any other person in the Academy, without that person's consent.

The Academy is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

Pupils breaking the rules of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, removal of content or referral to external agencies in the event of illegal activity. (See Prohibited Uses 1)

Additional Responsibilities for Pupils

Malfunctions or technical issues are not acceptable excuses for failing to complete homework, unless there is no other means of completion.

Pupils must not use their iPad in the Academy corridors unless for academic reasons and with the Teachers' permission. The iPad should then be used in a safe manner.

Completion of all class work remains the responsibility of the pupil.

If the iPad is lost, stolen, or damaged, the ICT Technicians must be notified immediately.

Prohibited Uses (not exclusive)

1. Accessing Inappropriate Materials – All material on the iPad must adhere to the E – Safety Policy**.** Students are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
2. Illegal Activities – Use of the Academy's internet/e-mail accounts for financial or commercial gain or for any illegal activity is not allowed.
3. Not respecting Copyrights – Students are not allowed to violate copyright.
4. Cameras – Students must use good judgment when using the camera. Students must agree that the camera will not be used to take inappropriate, illegal or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of the camera in toilets or changing rooms, regardless of intent no matter what the reason, will be treated as seriously breaking the Policy rules Use of the camera and microphone is strictly forbidden unless permission is granted by a teacher.
5. Posting of images/movies taken in the Academy to be uploaded onto the Internet into a public area is strictly forbidden, without the express written permission of the Teacher or a member of the Senior Leadership team.
6. Misuse of Passwords, Codes or other Unauthorized Access: Students are encouraged to set a passcode on their iPad to prevent other Students from misusing it.
7. Any students caught trying to gain access to another student's account, files or data will be subject to disciplinary action.
8. Unacceptable use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.
9. Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is not advisable. If you Jailbreak your iPad this might invalidate your insurance.

10. Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, bad language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
11. Individual Students are responsible for the setting up and use of any home internet connections and no support will be provided for this by the Academy.
12. Students should be aware of and abide by the guidelines set out by the Academy E Safety policy.
13. The Academy reserves the right to take away any iPad until the student's parents or carers can pick up) and search an iPad to ensure all the rules in this Responsible Use Policy have been followed.

Student Pledge for iPad Use

I will take good care of my iPad.

I will never leave my iPad about anywhere and go off without it.

I will never lend my iPad to others.

I will know where my iPad is at all times.

I will charge my iPad's battery every night

I will keep food and drinks away from my iPad because they may cause damage to the device.

I will not take apart any part of my iPad or attempt any repairs.

I will protect my iPad by only carrying it whilst it is in a case.

I will use my iPad in ways that are appropriate. (See Prohibited Use section 4)

I understand that my iPad can be inspected at any time and I do not have to be warned of such an inspection in advance.

I will only photograph or record people with their permission. (See Prohibited Use section 6)

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of staff or students anywhere at all in a public space on the Internet, unless I am asked to do so by my Teacher. (See Prohibited Use section)

Students must read the above and sign below:

I have read, understood and agree to abide by the terms of the iPad Acceptable Use Policy.

Name:

Signature:

Date:

Appendix 2

Personal Managed Device Acceptable Use Policy for Students

The policies, procedures and information within this document apply to all Mobile devices used by students in the Academy.

General Care and Guidance

Mobile Devices will need to be charged off site.

Syncing the iPad to iTunes or iCloud will be the student's responsibility.

Items deleted from a Mobile Device cannot be recovered.

The whereabouts of the device should be known at all times.

It is students' responsibility to keep their device safe and secure.

Devices belonging to other Students are not to be meddled with in any way.

If a device is found, it should be given to an IT Technician within the LRC

Students must use covers or cases that protect their device.

Do not leave the device in the academy or vehicles.

Students may not photograph any other person in the Academy, without that person's consent.

The Academy is not responsible for the financial or other loss of any personal files that may be deleted from a device.

Pupils breaking the rules of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, removal of content or referral to external agencies in the event of illegal activity. (See Prohibited Uses 1)

Additional Responsibilities for Pupils

Malfunctions or technical issues are not acceptable excuses for failing to complete homework, unless there is no other means of completion.

Pupils must not use their device in the Academy corridors unless for academic reasons and with the Teachers' permission. The device should then be used in a safe manner.

Prohibited Uses (not exclusive)

1. Accessing Inappropriate Materials – All material on the device must adhere to the E – Safety Policy**.** Students are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
2. Illegal Activities – Use of the academy's internet/e-mail accounts for financial or commercial gain or for any illegal activity is not allowed.
3. Not respecting Copyrights – Students are not allowed to violate copyright.
4. Cameras – Students must use good judgment when using the camera. Students must agree that the camera will not be used to take inappropriate, illegal or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of the camera in toilets or changing rooms, regardless of intent no matter what the reason, will be treated as seriously breaking the Policy rules Use of the camera and microphone is strictly forbidden unless permission is granted by a teacher.
5. Posting of images/movies taken in the academy to be uploaded onto the Internet into a public area is strictly forbidden, without the express written permission of the teacher or a member of the Senior Leadership team.
6. Misuse of Passwords, Codes or other Unauthorised Access: Students are encouraged to set a passcode on their device to prevent other Students from misusing it.
7. Any students caught trying to gain access to another student's account, files or data will be subject to disciplinary action.
8. Unacceptable use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.
9. Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, bad language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
10. Individual Students are responsible for the setting up and use of any home internet connections and no support will be provided for this by the Academy.
11. Students should be aware of and abide by the guidelines set out by the Academy E Safety policy.
12. The Academy reserves the right to take away any device until the student's parents or carers can pick up) and search a device to ensure all the rules in this Responsible Use Policy have been followed.

Student Pledge for iPad Use

I will take good care of my iPad.

I will never leave my iPad about anywhere and go off without it.

I will never lend my iPad to others.

I will know where my iPad is at all times.

I will charge my iPad's battery every night

I will keep food and drinks away from my iPad because they may cause damage to the device.

I will not take apart any part of my iPad or attempt any repairs.

I will protect my iPad by only carrying it whilst it is in a case.

I will use my iPad in ways that are appropriate. (See Prohibited Use section 4)

I understand that my iPad can be inspected at any time and I do not have to be warned of such an inspection in advance.

I will only photograph or record people with their permission. (See Prohibited Use section 6)

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of staff or students anywhere at all in a public space on the Internet, unless I am asked to do so by my Teacher. (See Prohibited Use section)

Students must read the above and sign below:

I have read, understood and agree to abide by the terms of the Mobile Device Acceptable Use Policy.

Name:

Signature:

Date: