E-Safety Policy

Date approved: 30.09.2020
Signed by Chair of Governors: Mr Nick Ager

Date approved: 30.09.2020
Signed by Headteacher: Mrs Kate Pereira

Reviewed: October 2023
Next Review: October 2024

St John Fisher Catholic High School

Policy and Procedures

Contents

E-Safety Policy

"I have come that they may have life and have it to the full"

John Chapter 10

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This E-safety Policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement and inappropriate use of AI technologies.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to

which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The E-Safety Policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT and E-Safety Coordinators.
- Regular monitoring of e-safety incident logs.
- Monitoring of filtering/change control logs and systems.
- Reporting to relevant Governors and/or committee(s) meetings

Senior Leadership Team (SLT)

The SLT are responsible for ensuring:

- The safety (including e-safety) of all members of the school community
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school E-Safety Policies and documents (in conjunction with e-safety co-ordinator)

- The school's Designated Child Protection Officers should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

Deputy Headteacher

The DHT takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Providing training and advice for staff which include ensuring their understanding of the systems we have in place for monitoring and filtering
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Co-ordinating and reviewing e-safety education programme in school

Business Manager

The Business Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements.
- The school's password policy is adhered to.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- The school keeps up to date with e-safety technical information.
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc) is regularly monitored in order that any misuse or attempted misuse can be reported to the SLT for investigation/action/sanction.

Currently St John Fisher Catholic High School engages the services of Breathe Technology for day-to-day support of the School's network and systems.

Teaching and Support Staff

In addition to elements covered in the Staff Acceptable Use Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP).
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the school's E-Safety and Acceptable Use Policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be informed of this via the school newsletter.

Education and Training

E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations - staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff/students should open the selected image and go to it's website to check for copyright.

Staff Training

- The Deputy Headteacher ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **Deputy Headteacher/Business Manager** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- Digital communications with students (e-mail, online chat, VLE, Teams, voice etc) should be on a professional level and only carried out using official school systems (see staff guidance in child protection policy and Staff Code of Conduct).
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems).
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with students) – but not for contact with parents/students.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.
- **Staff** should not be using personal mobile phones in school during working hours when in contact with students.
- Students should adhere to the rules and guidelines set out in the Mobile Phone Policy.

Social Networking Sites

Students and ex-students under the age of 18 will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using their personal equipment.
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Students/parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the wellbeing of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice will be sought from the relevant agencies, including the police if necessary.
- Students in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list is published to all staff on a termly basis, but can also be obtained from the data office or the child protection officers in school.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher or the ICT co-ordinator.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and twitter account which are used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Only school provided removable media should be used
- All files downloaded from the Internet, received via e-mail or provided on removable media (eg CD, DVD, USB flash drive, memory cards etc) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks
- Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff

Remote Learning

Please refer to Remote Learning Policy for further advice in terms of staff working in school or at home.

Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.
- The school only allows the SLT to access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems
- Staff will be required to use Swivel Secure system which requires two factor entry for accessing the school systems when working remotely.

Students

- Should only let school staff know their in-school passwords.
- Inform staff immediately if passwords are traced or forgotten. All staff should contact Student Services or ICT to change passwords.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Deputy Headteacher or Subject Leader for ICT.
- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment.
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the Heads of House or members of the Senior Leadership Team, depending on the severity of the incident.

- Breathe Technology will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems.
- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the Senior Leadership Team and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety Co-ordinator then the member of staff should report the issue to the Headteacher).

Incident Reporting

Any e-safety incidents must immediately be reported to the Deputy Headteacher (if a member of staff) or the Senior Leadership Team or Heads of House (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

Reviewed by Full Governing Body: December 2021

Next Review Date: October 2024 **Staff Member Responsible:** Deputy Headteacher

Appendix 1

ICT Acceptable Use Policy (Students)

The guidelines and rules in this Acceptable Use Policy have been written so that every student of St John Fisher Catholic High School can have safe, fair and reliable access to ICT to improve their learning and complete their school work. When using the school's ICT resources you should always be considerate of the consequences (intended or not) of your actions on other people. By following this policy you will not disrupt other users of the ICT resources and get the most benefit from using them yourself.

- I am responsible for how I use the school's ICT resources and will use them safely, responsibly and legally. I will not use them in a manner that will embarrass the school or its members.
- I will make sure I follow the advice given about staying safe when online. I will not share my personal details or the personal details of other people with anybody.
- I will not tell my password(s) to anybody else or allow them to use my account.
- I will lock or logoff my computer when leaving it and will only access resources and files I have been given permission to use.
- I will tell a member of staff when I see other people not using ICT safely or responsibly.
- I will only use the school's ICT and internet for tasks set by my teachers and will not allow copyrighted, undesirable, inappropriate or executable material onto the network either via the internet or removable storage.
- I will look after the school's ICT and use it carefully so that other users can use it effectively as well. I will not eat or drink next to a computer.
- I know that the school monitors my use of its ICT including any emails sent and received and what websites and network resources I access.
- I will not use any ICT (belonging to the school, myself or others) for the bullying or harassment of others.
- I will not try to get around the rules and safety systems on the school's ICT (for example by using proxy, mobile or foreign language sites) and will tell a member of staff if I notice anything that is unsafe.

Appendix 2

ICT Acceptable Use Policy (Staff)

1. I am personally responsible for my own use of ICT and upholding the standards laid out in this policy.
2. I will regularly take part in the school's e-safety training and ensure I am aware of the risks and opportunities the use of ICT presents.
3. I understand that ICT use in school is monitored including any personal or private communications made using the school's ICT resources.
4. I will protect my personal login information and will not allow other users to logon using my user name/password. I will lock or logoff workstations when leaving them unattended and will shut down the workstation that I am using at the end of each day.
5. I understand that the school's ICT systems are primarily intended for educational/professional use and that I will only use the systems for personal use within the school's policies.
6. I will use the ICT resources safely, responsibly and legally and will not use ICT in a manner that will bring the school, or its members, into disrepute.
7. I will report the misuse of ICT resources and unacceptable behaviour of others including but not limited to all illegal, harmful or inappropriate activities.
8. I will not access, copy, remove or otherwise alter another user's files without their express permission.
9. I will not attempt to install, copy or delete programs or amend any settings on the school network.
10. I will not attempt (without permission/consultation with IT Support) to make large uploads/downloads or store large files which might take up excessive amounts of internet capacity/network storage which will adversely affect the effective operation of the network or internet speed.
11. I will ensure that I adhere to copyright law and will not download, store or distribute any materials which are protected by copyright.
12. I will not try to upload, download or access, any unauthorised websites or materials which are illegal or contain inappropriate content such as pornographic, racist or offensive material. I will not try to use any programmes or software that might let me bypass the filtering/security systems in place to prevent such access.
13. I understand that data protection requires that any staff or student data is kept private and confidential and that I will ensure personal information about staff and students is kept safe and secure and avoid using it outside of the school network.
14. I will consider the needs of other ICT users and not use ICT resources in a way that diminishes the service for other users.
15. I will not engage in any activity that may compromise my professional responsibilities.
16. I will communicate with others in a professional manner and not use aggressive or inappropriate language.
17. I will not use any ICT resources (belonging to the school, myself or others) for the bullying or harassment of others.
18. I will not try to circumvent the ICT safeguards that are in place and will report any failings in the safeguards that I become aware of.

Appendix 3

Keeping Children Safe in Education September 2023, paragraphs 133 to 136

133 The following resources, plus many more listed in Annex B, may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools, https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- UK Council for Internet Safety (UKCIS)37 guidance: Education for a connected world, https://www.gov.uk/government/publications/education-for-a-connected-world
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people, https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors, https://www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings
- National Crime Agency's CEOP education programme: https://www.thinkuknow.co.uk/
- Public Health England: Every Mind Matters, https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview
- Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support. https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes

134 Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Online safety

135 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

136 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).