St John Fisher Catholic High School

E-SAFETY POLICY

Revision: July 2015
www.sjf.wigan.sch.uk

Table of Contents

E-SAFETY POLICY

Introduction and Aims

The use of ICT in school and at home has been shown to raise educational standards and promote pupil achievement. The purpose of the e-safety policy is to ensure safe and appropriate ICT use in school and at home. A wide range of legislation is relevant to this policy including the Communications Act, The Data Protection Act and the Computer Misuse Act.

Some of the risks and dangers associated with ICT 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.
- Illegal downloading/streaming of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning.

It is impossible to eliminate the risks outlined above. It is therefore essential, through good educational provision, to build pupils' resilience to these risks so they have the confidence and skills to deal with them. The school provides the necessary safeguards on its own network to manage and reduce the risks.

Roles and Responsibilities

Head teacher / Senior Leadership Group (SLG)

- The safety (including e-safety) of all members of the school community.
- Adequate training is provided.
- Effective monitoring systems are set up.
- That relevant procedures in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school's e-safety policy.
- The designated Child Protection Officer should be trained in e-safety issues.

E-safety Governor: Mr P Forshaw

- Regular monitoring of e-safety incidents.
- Report to the Pupil Progress and Pupil Welfare committee.

E-safety Officer: Miss P Mawdsley

- Day to day responsibility for e-safety.
- Liaise with staff, ICT technicians, e-safety governor and SLG on all issues related to e-safety.
- Ensuring that all staff are aware of the procedures to follow in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Receiving reports of e-safety incidents and create a log of incidents to inform future e-safety planning.
- Co-ordinate and review the e-safety education programme in school.

ICT Network Manager: Mr S Stevens

- The ICT network is secure and meets e-safety requirements.
- The filtering procedure is applied and updated on a regular basis.
- Regularly monitor the ICT network, remote access, e-mail etc. and report misuse or attempted misuse.
- Attends training, as necessary, on up-dating technical e-safety processes and procedures.

Teaching & Support Staff

- Read, agree and sign the staff acceptable use policy.
- Have up-to-date awareness of e-safety matters, policy and practices.
- Embed e-safety issues into the curriculum and other school activities.
- Ensure pupils understand and follow the pupil acceptable use policy.
- Ensure pupils understand the need to avoid plagiarism and uphold copyright regulations.
- Monitor ICT activity in lessons, extracurricular and extended school activities.
- Check internet sites are suitable, where possible, and that processes are in place to deal with unsuitable material found through internet searches.

Pupils

- Read, agree and sign the pupil acceptable use policy.
- Report abuse, misuse or access to inappropriate materials.
- Adopt good e-safety practice out of school.
- Understand that this e-safety policy covers their actions out of school, if related to their membership of the school.

Parents

- Read and agree to the pupil acceptable use policy.
- Ensure that their child understands the need to use ICT in an appropriate way.
- Be a positive role model in their use of ICT at home.
- Monitor the use of social networking and gaming sites and alert the relevant Head of year if they have concerns.
- Ensure that their child does not engage in any online behaviour that could have a detrimental impact on their membership of the school.

Education programme

E-safety is covered in the pastoral and assembly programme and is regularly revisited in ICT lessons and across the curriculum – this programme covers the safe and responsible use of ICT both within and outside of school.

Copyright

Pupils and staff should be aware of and uphold copyright regulations. Pupils are taught to do this in the following ways:

- Develop a good understanding of ICT research skills and the need to avoid plagiarism.
- Acknowledge the source of information used.
- If using a search engine for images, open the selected image and go to it's website to check for copyright.
- To be critically aware of content accessed on-line and the need to validate accuracy.

Training

- All new staff receive e-safety training as part of their induction programme.
- E-safety Officer to receive regular updates/training and review guidance documents.
- Governors are invited to take part in e-safety training and awareness sessions.

E-mail

- Digital communication with pupils (e-mail, blogs etc.) should be on a professional level only.
- E-mails should only be sent and received via the school's web-based system - under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

Social networking

- Pupils are not allowed on social networking sites at school.
- At home it is the parental responsibility (parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites).
- Staff users must not reveal the names of staff, pupils, parents or any other member of the school community on any social networking site.
- Pupils and parents should be aware that the school will investigate the misuse of social networking if it impacts on the well-being of other students or members of the school community.
- 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.

Digital images

- The school record of parental permissions must be adhered to when taking images of our pupils - a list can be obtained from the main office or the child protection officer in school.
- Images must not be taken using privately owned equipment.

Removable data storage devices

- Personal or confidential data must only be downloaded onto an encrypted or password protected data storage device and practices must fully comply with the Data protection policy.
- All files downloaded from the Internet, received via e-mail or brought into school on a data storage device must be checked for viruses using school anti-virus software before being opened or copied onto the ICT network.

Internet use

- Staff will preview any recommended websites before use.
- If Internet research is set for homework, specific sites that have previously been checked may be suggested - parents are advised to supervise any further research.
- Staff must actively monitor what pupils are viewing on the internet in lessons.
- Pupils must be made aware that all internet use at school is tracked and logged.
- The E-safety Officer, ICT Network manager and SLG have access to internet logs.

Passwords

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.
- Good practice is to change passwords at least every 3 months.
- Users should not use the same password on multiple ICT systems.
- Pupils must only let school staff know their in-school passwords and inform staff immediately if passwords are used by someone else or forgotten.

Use of school ICT device

- No software packages should be installed on school ICT equipment without permission of the ICT Network manager.
- Personal or confidential data should not be stored on local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- Staff must ensure any screens are locked before moving away from a computer during the normal working day to protect personal or confidential data and to prevent unauthorised access.

Monitoring

- All use of school internet access is logged.
- Internet logs are randomly but regularly monitored.
- If inappropriate use is detected it will be followed up by the E-Safety Officer, Heads of Year/Department or SLG depending on the severity of the incident.

Incident Reporting

- E-safety incidents involving a pupil must immediately be reported to the E-safety Officer.
- E-safety incidents involving a member of staff must immediately be reported to the Head teacher.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However, if infringements do occur they will be dealt with swiftly.

If any apparent or actual misuse appears to involve illegal activity this must be reported immediately to the Head teacher. Such matters will then be reported to the police.

Where misuse is not deemed to have been illegal it will be dealt with under the terms set out in the Behaviour policy for pupils and the Disciplinary policy for staff.

Legislation relating to e-safety

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual.

The Computer Misuse Act 1990 (sections 1 — 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include Racist, Xenophobic and Homophobic comments, messages etc.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour policy.