

E-SAFETY POLICY

Introduction

Our school community recognises the importance of treating e-safety as an ever-present serious safeguarding issue. It is important to protect and educate both pupils and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Ofsted reviews e-safety measures in schools and there are numerous Acts of Parliament which can be used to safeguard both staff and pupils in schools. The safeguarding aspects of e-safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review.

This policy links all the ICT, safeguarding and other policies and procedures to reflect how the school deals with e-safety issues on a daily basis. The documents referred to in this e-safety policy have been developed by various groups including:

- Governors.
- Headteacher/senior management team (SMT)/designated child protection staff.
- ICT technical support staff.
- Teachers and support staff.
- Parents/carers.
- Pupils.

Objectives and targets

This policy is aimed at making the use of electronic communication at St Bernard's Catholic Grammar School as safe as possible. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

Action plan

The school will deal with any e-safety incidents which arise by invoking this policy, other ICT policies and the associated behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school and take appropriate action.

The following sections outline:

- The roles and responsibilities for e-safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.

- How e-safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media.

Roles and responsibilities – governors

- Governors will ensure that appropriate filters and monitoring systems are in place on the school's ICT resources.
- Governors will ensure that pupils are taught about e-safety, for example through personal, social, health and economic education (PSHE) and through sex and relationship education (SRE).
- Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.
- Governors receive e-safety training/awareness sessions as part of their regular cycle of meetings.

Roles and responsibilities – headteacher and senior leaders

- The headteacher is responsible for ensuring the e-safety of members of the school community and will manage the education of pupils and training of staff in e-safety and awareness of potential radicalisation in pupils.
- The headteacher and another member of the senior leadership team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including the headteacher.
- The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of pupils 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, even though they may take place out of school, but are linked to membership of the school.

Roles and responsibilities – network manager

The network manager or technical support provider is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That appropriate filters and monitoring systems are in place.
- That the school meets the e-safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/e-safety policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.

- The headteacher is informed of any suspicions of pupils who may be becoming radicalised.

Roles and responsibilities – teaching and support staff

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy.
- They have read, understood and signed the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies eg staff e-mail, social media policies.
- They report any suspected misuse or problem to the headteacher/senior leader/ICT co-ordinator/class teacher/head of year as appropriate for investigation/action/sanction.
- Digital communications with pupils (email/personal learning environment (PLE)/voice) should be on a professional level and only carried out using official school systems.
- Pupils understand and follow the school e-safety policy and the pupil ICT acceptable usage policy.
- Pupils 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.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the e-safety issues pertaining to email and social media usage.
- They are alert to, and report to the headteacher, any suspicions of pupils who may be becoming radicalised.
- In lessons where internet use is pre-planned, pupils 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.

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

Roles and responsibilities – designated person for child protection/child protection officer

The designated person for child protection/child protection officer is trained in e-safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Suspicions of radicalisation.

Roles and responsibilities – pupils

Pupils:

- Are responsible for using the school ICT systems in accordance with the pupil ICT acceptable usage policy and agreement, which they will be expected to sign before being given access to school systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will 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 covers their actions out of school.

While regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. E-safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/PSHE/other lessons – this will include both the use of ICT and new technologies in school and outside school.

- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the pupil ICT acceptable usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

Roles and responsibilities – 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.

- Parents and carers will be responsible for endorsing (by signature) the pupil ICT acceptable usage agreement.

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 every opportunity to help parents understand these issues through:

- Parents' evenings.
- Newsletters.
- Letters.
- Website/PLE.
- Information about all relevant national/local e-safety campaigns/literature.
- Information about useful organisations /support services for reporting e-safety issues (see appendix 2).

Management of infrastructure

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the acceptable computer usage policy and any relevant LA e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually, by the Senior Management Team.
- All users will be provided with a username and password by the network manager.
- The 'master/administrator' passwords for the school ICT system, used by the network manager are also available to the headteacher or other nominated senior leader and kept in a secure place eg school safe.
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Sophos.
- Any filtering issues should be reported immediately to the network manager.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.
- Agreements are signed by members of staff in possession of school provided laptops regarding the extent of personal use that users and their family members are allowed on laptops and other personally owned devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. See the secure data handling policy and e-mail policy.

Curriculum

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to search the internet freely, eg using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff will ensure that they comply with the secure data handling policy by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users will be expected to know and understand school policies on email and social media
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.
- Any digital communication between staff and pupils or parents/carers (email, chat, PLE etc) must be professional in tone and content.

Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation of pupils.

Should any serious e-safety incidents take place, the appropriate external authorities will be informed (eg local area designated safeguarding officer, police etc).

Monitoring and reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate).
- Internal monitoring data for network activity.
- Surveys/questionnaires of pupils, parents/carers and staff.

The policy will be reviewed by the governors in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to e-safety.



APPENDIX 1

Acts of Parliament relevant to e-safety in schools

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 an offence liable, on conviction, to imprisonment. (This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.)

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 (eg using someone else's password to access files).
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (eg caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgment. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Counter-Terrorism and Security Act 2015 (section 26)

The prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)

It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years 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 data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyber-bullying/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/anti-bullying policy.

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.

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.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

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. Like the Racial and Religious

Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

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. Other laws already protect people from threats based on their race, nationality or ethnic background.

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.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (eg 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. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. 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.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

APPENDIX 2

Useful organisations/support services for reporting e-safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

On-line content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Media content inappropriate for children

If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through *ParentPort* at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.

Scams

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or <http://www.actionfraud.police.uk>. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

Getting help/advice: for young people

- *ChildLine*: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.

Getting help/advice: for parents

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk
- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 8pm, on 08451 205204 www.kidscape.org.uk.
- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'.

Contact details are: www.childnet.com, phone 020 7639 6967, email info@childnet.com.

- *UK council for child internet safety (UKCCIS)* has practical guides to help parents and others with internet safety www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.
- *Thinkuknow* has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

Getting help/advice: for teachers

- DFE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable teachers to raise concerns or questions directly with them.

Getting help/advice: for professionals working with children

- *Professionals online safety helpline*: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0844 3814772 (calls on this number are charged at local call rate).

Agreed by the Governor's Ethos Committee 3rd May 2017

Review Date: May 2019