BISHOP ULLATHORNE CATHOLIC SCHOOL

E-Safety Policy

2023*

***no change in policy just names of staff**

Review date: September 2025

BISHOP ULLATHORNE CATHOLIC SCHOOL

E-Safety Policy 2023

Our mission is to be an active Christian community of love and service where all feel they belong and are valued.

We will help each other to recognise the gift of God within us, to search for excellence and foster the development of our true self.

Our School E-Safety Policy is intended to help consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection / Safeguarding, Behaviour and Anti-Bullying, Preventing Extremism and Radicalisation policies. 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. We will, through our e-safety policy, ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

This policy's main aims are to protect pupils and staff in their use of technology and to clearly show the mechanisms to intervene and support any incident.

3 areas:

1. Content – illegal, inappropriate, harmful e.g. Pornography, violent games / films, age ratings, racist language, anorexia, suicide, hate sites, authenticity & accuracy of sites
2. Contact – harmful online interaction with others grooming, cyber-bullying, identity theft (Frape / hacking Facebook profiles), sharing passwords
3. Conduct – Personal online behaviour that can cause harm, disclosing personal information, reputation, health (amount of time spent online), sexting (SGII), copyright (e.g. film & music), conduct during online learning, peer on peer abuse.

Roles and Responsibilities

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Mrs Leanne Ward is the E-Safety and Child Protection/Safeguarding Governor.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator, Sarah Boyle.
- The Headteacher & Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Coordinator (Sarah Boyle)

- Has day to day responsibility for e-safety, working with the Child Protection / Safeguarding Officer role.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff

Network Manager (Mark Newell) / Technical staff:

The Network Manager / Technical Staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

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 Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher / E-Safety Coordinator / Officer for investigation / action / sanction
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

Child Protection / Safeguarding Designated Person / Officer (Fabia Hully)

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding 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

(NB. it is important to emphasise that these are child protection issues, not technical issues simply that the technology provides additional means for child protection issues to develop.)

Students / pupils:

Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / VLE and on-line student / pupil records
- Their children's personal devices in the school (where this is allowed)

Strategies for ensuring strong E-Safety

It is essential that 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. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
  The E-Safety Coordinator will provide advice / guidance / training to individuals as required.
- Pupils should be encouraged to come forward to speak to staff whenever they have worries and problems (as per Bullying policy)
- Online self-referral systems are in place to allow students to report any online abuse or concerns.

Dealing with E-Safety Issues (as per Bullying & Child Protection policies)

- Reports & incidents are treated with sensitivity, care and are fully investigated.
- Staff should deal with incidents immediately ensuring that disapproval of such behaviour is clear to all parties concerned.
- Staff must report incidents to Heads of Year who will decide upon appropriate course of action.
- Heads of Year keep Senior Staff informed.
- Any concerning online behaviour which appears to pose any risk to the safety of a child should be reported formally to the DSL immediately or as soon as possible.
- If a child's phone or electronic device is found to have abusive messages or content on it which may require external support (prevent, peer on peer abuse) then it is important that this information is not stored on school servers or directories.
- Staff in school are not allowed to retain or download any images from a child's phone with are sexually graphic or exposing in nature.
- Images or content that may refer to the school or feature school uniform but do not feature sexually explicit or suggestive material may be stored in school for investigative purposes.

Sharing nudes and semi nudes: how to respond to an incident

On occasion, it may be reported that a child has sent or received nude or semi nude images via their mobile device or similar internet enabled device. All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) and managed in line with the schools child protection policies. When dealing with an incident that involved nude or semi nude imagery the school will follow the guidance from the UKCISS:

- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Searching or monitoring a child's device

On occasion it may become necessary for a child's mobile or electronic device to be confiscated or searched. Any search can only be carried out by the designated safeguarding lead alongside a member of leadership team and the IT manager. When checking electronic devices,the school will adhere to the guidance provided by the Departmenr for Education, Searching Screening and Confiscation, July 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091132/Searching__Screening_and_Confiscation_guidance_July_2022.pdf

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk.

- The DSL in collaboration with a member of the leadership team and/or the IT manager may examine any data or files on an electronic device they have confiscated as a result of a search, if there is good reason to do so.

- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education.

- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable. In this instance the designated safeguarding lead must also be informed as soon as is possible.

- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State in the bullet points below:

- In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.

- In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

When dealing with E-Safety Issues our prime aims are:-

- To protect the child from harm
- To stop it / report it as necessary
- To ensure that there is no repetition

- To reassure the victim
- To punish the perpetrator
- To use strategies to prevent incidents recurring
- To ensure bystanders understand their role in preventing incidents

Parents should always be involved and be asked to play an active role in monitoring the situation.

All incidents of bullying must be subject to a school response.

APPENDIX I

Bishop Ullathorne Outstanding Practice:

All staff share responsibility for e-safety. Assemblies, tutorial time, citizenship, personal, social, health and education lessons, and an age-appropriate curriculum for e-safety all help pupils to become safe and responsible users of new technologies.

The school has a 'managed' system to improve knowledge and understanding of how to stay safe rather than a 'locked down' system. Pupils are given opportunities to learn how to assess and manage risk for themselves.

Senior leaders, governors, staff and families worked together to develop a clear strategy for e-safety. Policies are reviewed regularly (at least annually) in the light of technological developments.

Key Feature	Outstanding Practice	Evidence, Impact & Person Responsible	Next Steps
Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school. A high priority given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.	• New staff folders every September & for all new staff on joining (SGR) • Ongoing CPD delivered through INSET days • Policies shared in staff folders & school website (CBI, SGR & PC) • Policies & practice shared with parents & all stakeholders during Parent Evenings and on website (CBI & PC)	• Questionnaire for views of pupils and parents to develop e-safety provision.
Robust and integrated reporting routines	School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support. Remote monitoring tool presents report to DSL of all and any concerning language or search topics on school owned equipment	• Posters in rooms • Signposted in assemblies, ICT & CPSHE lessons • Parental guidance during workshops	• Anti-Bullying ICT / CPSHE Poster Competition • Insert into Student Diaries
Staff	All teaching and non-teaching staff receive regular and up-to-date training.	• CBI delivers all staff training on teacher days	• Audit the training needs of all staff during academic year

	One or more members of staff have a higher level of expertise and clearly defined responsibilities.	• updated policy for staff handbook • Mark Newell monitors activity	• Provide training to improve knowledge of and expertise in the safe and appropriate use of new technologies to all staff
Policies	Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, staff and parents.	• All staff aware of policies & procedures (CBI)	• Policy ratified by governors, inserted into staff handbook & published on website.
Education	An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.	• Students know E-Safety issues through assemblies, national events, ICT & CPSHE lessons • Students rewarded through poster competition	• Community and self-management rewarded through SLG ACE points system • Competitions rewarded through assemblies and prizes
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.	• Mark Newell monitors activity & reports as necessary	
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.	• CBI measures impact of training, student learning & parental engagement through questionnaire result analysis	• Stakeholder questionnaires completed, reviewed & analysed (cyclical & on-going)

Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998. Any professional communications between the setting and clients that utilise technology should: • take place within clear and explicit professional boundaries • be transparent and open to scrutiny • not share any personal information with a child or young person.	• IT Systems team ensure legal obligations are met	• On-going staff training

- Children integral to policy production
- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Train ALL staff systematically & monitor impact systematically.
- Provide lists of what current risks are and what resources are available to help them keep pupils and themselves safe online.
- Parents' e-safety advice provided during information evenings
- Raising awareness through school website & newsletters
- Regular and relevant e-safety resources offered to parents, often via accessible platforms such as social media.
- There is progressive, planned e-safety education across the curriculum, within KS3 & KS4 ICT & CPSHE
- Headteacher and other leaders deliver assemblies to all year groups
- Continue to work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Continue to use managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- Continue to review & update an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Work with partners and other providers to ensure that pupils who receive part of their education away from school are e-safe.
- Systematically review and develop e-safety procedures & policies, including training, to ensure that we have a positive impact on pupils' knowledge and understanding.
- Personal data is secured and/or encrypted on Arbor.

- Security of passwords is strong and passwords are not shared or common.
- Internet is filtered & monitored by Coventry City Council.
- Staff are trained regularly & children are aware of how to report problems.

APPENDIX II:

Glossary

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/

In addition, the following terms used in this document are explained below

360 degree safe E Safety Award	SWGfL's online self-review tool for school improvement in online safety www.360safe.org.uk.
AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and mobile phones.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.

Profile	Personal information held by the user on a social networking site.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self-generated indecent images (often referred to as “sexting” –see above)
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
YouTube	Social networking site where users can upload, publish and share video.

Further information

UKCICIS – Online Safety in Education (December 2015)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517217/Online_Safety_in_Education_December_2015__2_.pdf

Teaching online safety in schools (Department for Education January 2023)

https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Keeping children safe online (NSPCC)

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Websites

UK Council for Child Internet Safety (UKCCIS); https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Child Exploitation and Online Protection Centre (CEOP); http://ceop.police.uk/

UK Safer Internet Centre; http://www.saferinternet.org.uk/

Childnet International; http://www.childnet.com/

SWGfL (South West Grid for Learning); http://www.swgfl.org.uk/

Parentzone; http://parentzone.org.uk/

Kooth - https://www.kooth.com/