BLESSED HUGH FARINGDON CATHOLIC SCHOOL

E-SAFETY POLICY

All that happens in Blessed Hugh Faringdon Catholic School occurs within the context of the school's Mission Statement (in accordance with the Trust Deed for the maintenance and advancement of the Catholic religion).

Written: June 2018
Updated: September 2024
Adopted: September 2024
Persons Responsible: Headteacher and Governing Body
Committee: Curriculum and Personnel
Review: 3 Yearly
Review Due: September 2027

As a Catholic school, founded on, and committed to upholding the teaching of the Church, we believe that Jesus is present in the day-to-day life of our community and that each member of our community has a divine origin and an eternal destiny. In discharging our responsibilities, we are guided by the principles of Catholic social teaching [CST], in which the following core values are constituted: dignity, solidarity, the common good, the option for the poor, the promotion of peace, care for creation, the dignity of work and the value of participation in society. These principles are demonstrated in our core, and wider, curriculum, in our care of students, in our work with the disadvantaged and in the outward-facing approach to our local community, our nation and to the world. As our moral compass, CST guides us in all our school activities, including the formulation, upholding and reviewing of school policies.

Blessed Hugh Faringdon Catholic School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Introduction

E-safety is a whole-school priority and covers the Internet, mobile phones and any other electronic communications technologies. Lockdown has highlighted the dangers of social media and we take steps to educate our students in appropriate social media interactions and use (see current Child Protection and Safeguarding Policy) It is known that some adults and young people will use these technologies to distress or harm children. This ranges from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children to be mindful of the risks and for the school to ensure that all members of

the school community are educated regarding the symptoms and the actions to take. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full positive potential. This policy aims to provide guidance for ICT activity in school providing a good understanding of its appropriate use as a point of reference for conduct on-line within and outside school.

Cyber-bullying is serious and is managed through our behaviour and safeguarding procedures. There is specific reference to cyber-bullying in our Anti-bullying Policy.

Roles and Responsibility The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Key responsibility lies with the: • Headmaster • Designated Safeguarding Lead (DSL) • Key Stage 3 Deputy Designated Safeguarding Lead (DDSL) • Key Stage 4/5 Deputy Designated Safeguarding Lead (DDSL) • Designated Safeguarding Member of the Governing Body.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Governors receive regular up-dates via the link Governor, DSL and the Safeguarding section of the Headteachers' Report to Governors. Governors are invited to participate in e-safety training as and where appropriate to their role. This may be offered face to face or on-line.

Senior Leaders

The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community; The DSL ensures all staff are aware of the procedures to be followed, in the event of an e-safety incident taking place, monitors the work of the DDSLs to address student issues of misuse of technology and ensures school processes are being followed. Daily alerts from Securus (Internet Security Software) are monitored by the DSL and acted upon by the DDSLs. Evidence of misuse of personal technological equipment is also investigated and acted upon. Secure records are kept. Senior Leaders are aware of the procedures to be followed in the event of an e-safety allegation being made against a member of staff.

Deputy Designated Safeguarding Leads

To take day to day responsibility for acting upon e-safety issues and maintaining records;

- Liaise with the Local Authority;
- Liaise with the police;
- Liaise with school's Network team;
- Liaise with Securus;
- Liaise with parents and carers;
- Report regularly to the DSL.

Network Manager

The Network Manager is responsible for ensuring that:

- the school's technological infrastructure is secure and is not open to misuse or malicious attack;
- the school meets required safety technical requirements and any Local Authority E-Safety Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy; the filtering policy is applied;

- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- the use of the network / Internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the Headmaster, DSL/DDSLs;
- monitoring software / systems are implemented and updated as agreed with the Headteacher.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that they have an up to date awareness of e-safety matters and the current school e-safety policy and practices;

- as a new member of staff, they have read, understood and signed the Staff Acceptable Use Agreement (AUA). Records are kept by our HR Officer;
- they report any suspected misuse or problem to the appropriate member of the safeguarding team for investigation / action / sanction;
- all digital communications with students / parents / carers are at a professional level and via the school system only;
- e-safety considerations are embedded in all aspects of the curriculum and other activities where appropriate;
- students understand and follow the e-safety and Acceptable Use Agreements and that parents/carers have confirmed this understanding;
- students have a good understanding of appropriate research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies regarding these devices;
- where Internet use is pre-planned, for lessons, students are guided to sites that have been checked as suitable and that the Network Team is advised of any unsuitable material that is found in Internet searches such that access to it can be blocked.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement;
- must have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and take advice where unclear;
- must understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- are expected to know and understand policies on the use of mobile devices and digital cameras;
- are expected to know and understand policies on the taking / use of images and on cyberbullying. Students using any technology to make, or attempt to make, covert audio or visual recordings of other students, staff or visitors will be in serious breach of the behaviour policy. This constitutes a gross invasion of privacy as well as a misuse of technology.
- 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 covers their actions out of school, if related to their membership of the school
- Staff are required to read the E-safety Policy and digitally sign to confirm.

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/carers must sign the Student Acceptable Use Agreement on an annual basis having ensured their child understands its requirements.

The school ensures that any updates are conveyed via Heads-Up and the school website as appropriate.

Evaluating Internet Content

It is important that students learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy where computers are used to support learning in lessons. It is expected that students are taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- to use age-appropriate tools to search for information online;
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism very seriously. If a piece of coursework is found to be plagiarised, the student risks being prohibited from completing the relevant external examination. The school takes steps to filter Internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, then the URL must be reported to the Network Manager. Any material found, by members of the school community, that is believed to be unlawful is reported to the appropriate agencies via the safeguarding team. Regular software and broadband checks take place to ensure that filtering services are working effectively.

Managing Information Systems

The school is responsible for reviewing and managing the security of computers and Internet networks and takes the commitment to protect school and personal data seriously. This means protecting the school network, as far as is practicable, against viruses, hackers and other external security threats. The security of the school

information systems and their users is subject to regular review and virus protection software updated accordingly. Steps taken to secure our computer systems include:

- ensuring that all personal data sent over the Internet or taken off site is encrypted;
- making sure that unapproved software is not downloaded to any school computers;
- regular checking of files, held on the school network, for viruses;
- the use of user logins and passwords to access the school network;
- Tablet computers used by teaching and support staff off-site are password protected;
- Other Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

More information on protecting personal data can be found in the current Data Protection Policy.

Published Content and the School Website

The school website is considered a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up to date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain and can be viewed by anyone online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published and data contained for internal use is password protected with limited access. Policy and guidance on safe use of student's photographs and work Photographs and student's work bring our school to life, showcase our student's talents, and add interest to publications that represent the school both online and in print. However, the school acknowledges the importance of safety precautions to prevent the misuse of such material. We believe that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community. However, we would also like to use photographs and videos of the school and its students externally for promotional purposes (in the public domain) and in order to promote the good educational practice of the school. In accordance with the Data Protection Act and our Data Protection Policy we will do this, only, with parent/carer consent. On admission to the school parents/carers will be asked to "opt out" of allowing the use of images of their child in the following ways:

- all school publications;
- on the school website;
- in newspapers as allowed by the school; • in videos made by the school or in class for school projects.

Using photographs of individual children

Most people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, in some cases, the intention is abuse. Thus, safeguards are in place. It is important that published images do not

identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or engaged in school activities without the school's permission. The school follows good practice principles on the use of photographs of individual children:

- A list of students whose parent/carer has not given permission is maintained on file.
- Electronic and paper images are stored securely.
- Images are carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse will not be used. • For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or tutor group.
- Events recorded by family members, of the students, such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will always wear identification, and will not have unsupervised access to the students.

For more information on safeguarding in school please refer to our Safeguarding Policy.

Complaints regarding misuse of photographs or video:

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

Social networking, social media and personal publishing

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of the potential dangers which have been further highlighted over the lockdown period. Personal publishing tools including blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes are amongst the most obvious sources of inappropriate postings and interactions leaving students vulnerable to being contacted by someone who intends harm. Via our PSHE Programme, tutor periods and assemblies we educate students so that they can make their own informed decisions and take responsibility for their conduct online. The school follows established rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- The school has installed effective filters on the ICT system to block known inappropriate websites.
- Any accessible sites that are to be used in class must be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum must be password-protected and run with the approval of the Headmaster and safeguarding team.
- Due care and attention is exercised in selecting photographs for our Twitter Feed.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school, at all times, and must act appropriately.
- Completion of the Introduction to Safeguarding on-line course and the requirement to read the E-Safety Policy and all related policies, annually, and digitally sign to confirm they have done so ensures that all staff are aware of requirements.
- The use of any video or audio-conferencing applications is in line with the Remote Learning Policy and with due care for safeguarding. This includes remote lessons, meetings and Parents' Evenings. Where they are recorded it is with the knowledge of the participants.

Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Issues surrounding the possession of these devices include:

- an increased risk of cyberbullying;
- potential access to inappropriate Internet material;
- the risk of theft, loss or damage to the device;
- potential inappropriate use. For example, to take photos and record dialogue (unlawful).
- The school advocates that ,where parents permit students to bring their mobile phone into school, it must be switched off and not used during the school day or when on the school site.
- Staff will confiscate mobile phones where students misuse them, their actions will be investigated, and the appropriate actions taken in line with our safeguarding procedures. Parents will be contacted.

Responsibility: Blessed Hugh Faringdon Catholic School accepts no responsibility for theft, loss or damage relating to personal phones/devices other than those which have been handed into the school office for safekeeping.

Staff

For safeguarding and data protection reasons, staff should not use their own personal devices to contact students or parents, either in or out of school time, unless in an absolute emergency. In such instances care should be taken to block personal phone numbers prior to making the call.

- Staff must limit the taking of photos or videos of students (for example on school trips), on personal devices, to internal use and respect the wishes of parents who have withdrawn permission for the school to photograph or video their child.

- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy will be investigated and may result in disciplinary action against that member of staff.

Cyberbullying: Our Anti-Bullying Policy contains a very clear statement regarding cyberbullying, the seriousness the school places on any such behaviours and the process to follow. Please read this section of the Anti-bullying Policy for further guidance.

Managing Emerging Technologies: Technology is progressing rapidly, and new technologies are constantly being developed. The school will risk-assess any new technologies, along with their educational benefits, before deciding how to proceed. Clear guidance will then be published in the form(s) appropriate to ensure that staff, students and parents/carers have a full and complete knowledge and understanding of our requirements and expectations. Following the August 2024 central government announcement regarding work to develop appropriate Artificial Intelligence (AI) platforms and resources to reduce teacher workload, we will keep abreast of developments and adjust accordingly with the wellbeing of our staff and students at the heart of decision-making in this regard.

Protecting Personal Data: We are fully compliant with the requirements of GDPR and the use and sharing of data is monitored carefully. There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information to external authorities, for example, our local authority, OfSTED, the police or Social Services. GDPR guidelines are followed in these circumstances. For more information please refer to the schools' current Data Protection Policy.

Unsuitable / inappropriate activities: The filtering and monitoring guidelines are followed. Some Internet activity e.g. accessing child abuse images or disturbing racist material is illegal and is banned from school systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. Below is a range of activities which may be legal but are inappropriate in a school context either due to their nature of because they are age inappropriate. These are monitored internally, by our network team who have ensured filters are in place, and via the daily Securus captures are not allowed in school and include the following:

- pornography;
- promotion of any kind of discrimination;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- using school systems to run a private business;
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- infringing copyright;

- revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords;
- creating or propagating computer viruses or other harmful files;
- on-line gaming both educational and non-educational;
- on-line gambling;
- use of social media without permission;
- use of messaging apps without permission;

Responding to incidents of misuse: It is essential that any incidents are dealt with, promptly and in the appropriate manner as indicated below. Incidents which are against the law. Such incidents are reported to the police.

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy.

Staff are required to read and sign the Acceptable Use Form on arrival in the school. However, there may be times when infringements of the policy could take place, through careless irresponsible or deliberate misuse. All instances will be investigated, and the appropriate actions and monitoring ensured. Should the content being reviewed include images of child abuse then it will be referred to the police immediately. In the event of suspicion of inappropriate behaviours of a staff member, this procedure should be followed:

- The incident must be reported to the Headmaster who will consider the issue, based on the evidence, and may request that the DSL (Designated Safeguarding Lead) conducts an investigation following the due process. Records should be kept securely. Once fully investigated the Headmaster/DSL should judge whether this concern has substance or not. If so, an appropriate action will be taken and could include the following;

- Internal response or discipline procedures;
- Involvement of the Local Authority;
- Involvement of the Police.

Where investigations uncover evidence of the following the police will be contacted:

- ‘grooming’ behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or material.

This policy demonstrates Blessed Hugh Faringdon Catholic School’s commitment to ensuring the E-Safety of our students and community.