SACRED HEART HIGH SCHOOL

E-SAFETY POLICY

OCTOBER 2019

To be reviewed October 2020

This Policy should be read in conjunction with all other Sacred Heart High School Policies

Contents

1 INTRODUCTION

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Sacred Heart High School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Sacred Heart High School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

This E-Safety Policy is part of the School Development Plan and relates to other policies such as the Safeguarding and Child Protection Policy; the Computer Resources Policy and Acceptable Use Agreement; the Anti-Bullying Policy; Use of Images of Children Policy; etc.

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students/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, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Disclaimer

Sacred Heart High School makes every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable. Nevertheless, SHHS and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

The school will appoint an e-safety coordinator. In some cases this will be the Child Protection Liaison Officer as the roles overlap.

2 POLICY DECISIONS

2.1 Authorising Internet Access

All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Pupils at Sacred Heart High School must apply for internet access individually by agreeing to comply with the Computer Resources Policy and Acceptable Use Agreement.

Any person not directly employed by the school will be asked to sign an 'Acceptable Use Policy' before being allowed to access the internet from the school site.

2.2 Assessing Risks

The school will complete on an annual basis an E-Safety audit carried out by the e-safety co-ordinator.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

With reference to the above staff must inform the head teacher/E-Safety co-ordinator immediately if inappropriate material is accessed or appears unintentionally.

The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Staff are to inform the head teacher/E-Safety co-ordinator of any unsuitable material.

2.3 Handling E-Safety Complaints

Complaints of internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

2.4 Community Use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the school e-safety policy.

3 TEACHING & LEARNING

A planned e-safety programme should be provided as part of Computing and ICT/PSHE/ and embedded within other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

3.1 Why internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The school internet access is provided by LGfL which includes filtering appropriate to the age of pupils.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information appropriately to a wider audience.

3.2 Curriculum

Pupils are responsible for using the school ICT systems in accordance with the Acceptable Use Policy, which they will be expected to sign before being given access to school systems and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Pupils will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon. For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home.

For children with social, family or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Pupils will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

Key e-safety messages should be reinforced as part of a planned programme of assemblies, tutorial/pastoral activities and subject curriculum activities as part of ICTAC.

Pupils should 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.

Staff should act as good role models in their use of ICT, the internet and mobile devices.

In lessons where internet use is pre-planned, it is best practice that 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.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

4 MANAGING INTERNET ACCESS

4.1 Information System Security

School ICT systems security will be reviewed annually.

Virus protection will be updated regularly.

Security strategies will be discussed with the Local Authority, LGfL and any other services as required due to the development of new and existing technology.

4.2 E-mail

The school provides staff and pupils with an email account for their professional use.

Pupils must immediately tell a teacher if they receive any offensive e-mails.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The forwarding of chain letters is not permitted.

The school will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

Staff are made aware of the responsibility when sending emails either internally or to external organisations, pupils or parents that they ensure it is written carefully.

4.3 Published content and the school web site

The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The email contact address will be info@sacredh.lbhf.sch.uk.

The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Uploading of information is restricted to our website authorisers such as the IT Manager and Digital Media Co-Ordinator.

The school web site complies with the statutory DfE guidelines for publications.

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

We do not use embedded geodata in respect of stored images.

We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

4.4 Publishing pupils' images and work

Photography by staff in school, during school activities, on school trips and visits may be used in the curriculum and displayed within the school, on the school website or at parents' evenings to illustrate the work of the school.

The school will keep a register on the MIS system of parents who have agreed for their children's photographs to appear in school publicity and on the website. This will be updated annually as part of the data checking process.

Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Photographs are 'personal data' as far as data protection legislation is concerned and must be used responsibly.

It is not appropriate for adults to take photographs of children for their personal use.

It is also not appropriate for adults to take photographs using personal equipment and storage, such as mobile phones or tablets.

Where the school has no record of receiving such parental consent, it should be deemed that consent has not been given.

The school will only take and use images that are appropriate and are considered to not be open to misuse.

When taking photos, it is preferable to use group pictures.

If an image of a child is used, the child's name will not be published. If a name is published, no image will be used without specific consent.

Children will be made aware of why their picture is being taken and how it will be used.

Children will be given the option to not have their image used if they are the sole focus of the picture.

Children and parents should be encouraged to recognise the value of group photographs or recordings of school events.

Images will be kept securely in the staff area. No unauthorised access will be given to these images.

Images of children from the school will not be used to illustrate controversial subjects.

4.5 Social networking and personal publishing on the school learning platform.

The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. This control may not mean blocking every site it may mean monitoring and educating students in their use.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils must not place personal photos on any social network space provided in the school learning platform.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities; however it does present dangers for primary and secondary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

4.6 Managing filtering

The school will work in partnership with LGfL and Hammersmith and Fulham Council to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

A log of any incidents may be useful to identify patterns and behaviours of the pupils.

4.7 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.

Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.

Staff will use a school phone where contact with pupils is required.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

4.8 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

4.9 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

5 COMMUNICATIONS POLICY

5.1 Introducing the E-Safety Policy to Pupils

Appropriate elements of the e-safety policy will be shared with pupils.

E-safety rules will be posted in all networked rooms.

Pupils will be informed that network and internet use will be monitored.

Curriculum opportunities (as outlined in page 2) to gain awareness of e-safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as students become more mature and the nature of newer risks can be identified.

5.2 Staff and the E-Safety Policy

All staff will be given the School e-safety Policy and its importance explained.

All staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.

Staff should be aware that internet traffic and computer use can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

5.3 Enlisting Parents' Support

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents should be given e-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.
- Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation.

6 DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER POLICY

6.1 Strategic and operational practices

The Head Teacher is the Senior Information Risk Officer (SIRO) who reports to the Schools' Data Protection Officer (DPO).

The School's DPO can be contacted via email at the following address

DPO@sacredh.lbhf.sch.uk.

Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.

Staff know who to report any incidents where data protection may have been compromised.

All staff are DBS checked and records are held in one central record.

The school follows LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

Have an approved remote access solution so identified staff with the approved level of access can access sensitive and other data from home, without need to take data home.

Staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

6.2 Technical Solutions

Staff have a secure area(s) on the network to store sensitive documents or photographs.

Staff are required to log-out of systems when leaving their computer.

All servers are in lockable locations and managed by DBS-checked staff.

The school complies with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any

protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

7 RATIFICATION

This E-Safety Policy has been written by the school, building on best practice and government guidance.

The Policy has been approved and ratified by the Headteacher and Ethos Committee of the Governing Body on Wednesday 16 October 2019. The Policy will be reviewed for October 2021.

Mrs M Doyle
Headteacher

Dr Michael Phelan
Acting Chair of Ethos Committee

APPENDIX 1: E-SAFETY AUDIT

Committee	Does the school have a nominated e-safety Committee?	Y/N
	The e-safety Coordinator is:	
	The Child Protection Liaison Officer is:	
	The responsible member of the Governing Body is:	

Policies	Does the school have an E-safety Policy that allies with the DfE guidance?	Y/N
	The school e-safety policy was last updated/reviewed on:	
	The school e-safety policy was agreed by governors on:	
	The policy is available for staff at:	
	The policy is available for parents/carers at:	
	Do all staff sign an Acceptable Use Policy on appointment?	Y/N
	Have all pupils signed (where appropriate) the School's e-safety Rules?	Y/N
	Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
	Do parents/carers sign and return an agreement that their child will comply with the School e-safety Rules?	Y/N

Education and CPD	Are regular e-safety updates and training provided for all staff and governors?	Y/N
	Are regular e-safety updates and training provided for parents and other stakeholders?	Y/N
	Have appropriate teaching and/or technical members of staff attended training on the school's filtering system?	Y/N
	Does the school carry out pupil voice activities to ascertain new risks they may be experiencing?	Y/N
	Has e-safety been embedded across the curriculum in all year groups?	Y/N
	Have e-safety materials and resources been obtained for children to access e-safety education (e.g. from CEOP, Thinkuknow, Know it All)	Y/N

E-safety risks	Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	Y/N
	Is personal data collected, stored and used according to the principles of the Data Protection Act 2018 and GDPR?	Y/N
	Is internet access provided by an approved educational internet service provider which complies with DfE requirements (e.g. LGfL, RM, EasyNet, Regional Broadband Consortium, NEN Network)?	Y/N

Response Procedures	Is there a clear procedure for a response to an incident of concern?	Y/N
	Is there a log and process to track incidents and trends.	Y/N
	Are all staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	Y/N