

TITLE OF POLICY:	E-SAFETY POLICY
PREPARED BY:	BEN TIPTON
DATE POLICY PRESENTED TO GOVERNORS:	AUTUMN 2024
DATE DUE FOR REVIEW:	AUTUMN 2026

Sacred Heart R.C. Primary School WESTHOUGHTON E-SAFETY POLICY

Our e-safety Policy has been written by the school and has been adapted from the Kent's Children Families and Education Directorate draft policy, following Becta guidance. It has been agreed by the Senior Leadership & Management Team and approved by the Governing Body. It will be reviewed annually.

Writing and reviewing the e-safety policy:

The e-Safety Policy is part of the School Improvement & Development Plan and relates to other policies including those for Computing, Anti-Bullying and for Child Protection.

The school will appoint an e-Safety coordinator. [In many cases this will be the Designated Child Protection Coordinator as the roles overlap];

Our e-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the Senior Leadership & Management Team and approved by the Governing Body;

The e-Safety Policy and its implementation will be reviewed annually.

Safety Audit:

This quick self-audit will help the Senior Leadership & Management Team (SLMT) assess whether the e-safety basics are in place to support a range of activities.

Does the school have an e-safety Policy that complies with Becta guidance?	Yes
Date of latest update:	Autumn 2024
The policy was agreed by governors on:	The policy was agreed by governors on: Autumn 2024
The policy is available for staff at: Online:	Online : school website
And for parents at: Online:	Online: school website
The Designated Child Protection Coordinator is:	The Designated Child Protection Coordinator is: Sam Dootson
The e-safety Coordinator is:	Mr B Tipton
Has e-safety training been provided for both students and staff?Yes	Yes
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the school e-safety rules?	Yes
Have school e-safety rules been set for students?	Yes – annually [Autumn Term]
Are these rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational internet service provider and complies with DfE requirements for safe and secure access	Yes
Has an ICT security audit been initiated by SLMT, possibly using external expertise?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

Teaching and learning:**Why internet use is 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.

Ensure that internet use will enhance learning:

The school internet access is provided by Bolton Council and 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 effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content:

Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law;
Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
Sanctions for inappropriate use of the internet will be explained to the children.

Managing Internet Access:**Information system security:**

School ICT/Computing systems capacity and security will be reviewed regularly;
Virus protection will be installed and updated regularly;
Security strategies will be discussed with the Local Authority.

E-mail:

Pupils and staff may only use approved e-mail accounts on the school system;
Pupils must immediately tell a teacher if they receive an offensive e-mail or message via instant messaging systems or via the school learning platform whilst in school;
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 e-mail address or from within the learning platform and will be monitored;
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
E-mails sent that include details of pupils must be sent securely by encrypting the email before sending it. The forwarding of chain letters is not permitted.

Published content and the school website

Any information that can be accessed outside the school's intranet should be classed as published whether electronic or paper format.

Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published;
The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Staff and pupils using digital cameras, video recorders or sound recorders, including radio station and film studio, will ensure that they inform others before recording them and always use equipment in a respectful manner;
Photographs that include pupils will be selected carefully and will not include details of full pupil names alongside photographs;
Pupils' full names will not be used anywhere on the website, school Facebook page, school Twitter or learning platform including in blogs, forums or wikis, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, Facebook, Twitter or other media sharing platforms.

Social networking and personal publishing on the school learning platform

Sacred Heart has its own Facebook page and Twitter account. The school will publish details of activities and achievements taking place within school to inform and celebrate. Pupils' full names will not be used anywhere on the school Facebook, Twitter or learning platform including in blogs, forums or wikis, particularly in association with photographs. Photographs that include pupils will be selected carefully and will not include details of full pupil names alongside photographs;
Bolton Council will normally block / filter access to social networking sites for pupils (other than those within the UniServity learning platform) unless short term access is required for a specific educational project;
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 unless for a particular project approved by the school e-safety coordinator;
Pupils should be advised on security and encouraged to set strong passwords, deny access to unknown individuals and how to block unwanted communications;
Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

The school will work in partnership with Bolton Council to ensure systems to protect pupils are reviewed and improved;
If staff or pupils discover an unsuitable site, it must be reported to school immediately so appropriate action can be taken.

Managing video conferencing

IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet;
Pupils should ask permission from the supervising teacher before making or answering a video conference call, including calls originating within the learning platform;
Video conferencing will be appropriately supervised for the pupils' age.

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 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;
Staff will be issued with a school phone where contact with pupils families is required (such as a trip or residential).

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions:

Authorising Internet access

All staff must read and sign the 'Staff Information Systems Code of Conduct' 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. This record will be kept up to date;
Pupils must apply for internet access individually by agreeing to comply with the 'Responsible Internet Use Statement';
Parents will be asked to sign and return a consent form.

Assessing risks

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 Bolton Council can accept liability for the material accessed, or any consequences of Internet access;
Any inappropriate access whether intentional or unintentional will be reported to the e-safety co-ordinator and to the LA where necessary;
The school will audit ICT/Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by a senior member of staff and where appropriate we will inform the LA;
Any complaint about staff misuse must be referred to the Head teacher immediately;
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 on request.

Communications Policy:

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year;
Pupils will be informed that network, internet and learning platform use will be monitored and can be monitored and traced to the individual device or login. Staff and the e-safety policy All staff will be given the School e-safety Policy and its importance explained;
Staff should be made aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential;
The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Enlisting parental support

Parents' attention will be drawn to the school e-safety Policy in newsletters, published school materials and on the school website / learning platform.

MONITORING

The Governing Body will monitor and review this policy annually.

Policy agreed by Governing Body **Autumn Term 2024**

Policy to be reviewed **Autumn Term 2026**