Online Safety Policy 2023-25

Mission Statement

Guided by truth, respect and compassion; we share in building upon every individual's foundation, nurturing a love of learning in preparation for tomorrow's society, with Jesus at the heart of all we do.

Governing Body with Responsibility	Resources
Agreed by Governors on	21/11/2023
Chair's Signature	
Staff Member Responsible for Review	SBM
Date for Review	November 2025

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside the school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

This policy follows the Department for Education's advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet

Designated Safety Lead

The DSL takes "lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place".

- Ensure an effective whole school approach to online safety as per KCSIE
- Stay up to date with the latest trends in online safeguarding

- Communicate regularly with SLT and the Safeguarding Governor to discuss current issues (anonymised), review incident and filtering logs and discuss how filtering and monitoring work has been functioning/helping.
- Ensure all staff are aware of the procedures to be followed in the event of an online safety incident and that these are logged in the same way as any other safeguarding incident.

This list is not intended to be exhaustive.

The Headteacher

The headteacher will:

- Ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Work with the IT Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy and the Anti Bullying Policy
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Governing Body

This list is not intended to be exhaustive.

The School Business Manager

The SBM is responsible for:

- Collaborating regularly with the Network Manager (MM-ICT), Merton's School IT department and the SLT to help school make key strategic decisions around the safeguarding elements of technology.
- Ensuring that the filtering and monitoring systems are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Working with the Headteacher to ensure the school website meets statutory DfE requirements.

This list is not intended to be exhaustive.

The IT Lead

The IT Lead is responsible for:

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that E-safety is fully integrated across the curriculum.
- Organising and leading E-safety Day each year
- Monitoring the quality of the E-safety curriculum.
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and the Anti Bullying Policy

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Pupils

Pupils are expected to:

- Read, understand and adhere to the pupil acceptable use policy

Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Appropriate Filtering and Monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" webfiltering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring and there is a designated Governor with responsibility for filtering and monitoring.

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking.

They can submit concerns at any point using the school's Reporting Web Filtering Concerns Google form.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training is provided.

At Sacred Heart children do not use Google when searching the internet. They use https://www.safesearchkids.com/, which is powered by google - but filtered to ensure safe searching (where possible).

- web filtering is provided by WebScreen filtering (LGfL) on school site
- changes can be made by Damian Fearon (IT Lead), Jane Pringle (SBM) and MM-ICT IT support
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from Merton Schools' ICT (Derek Crabtree and Mark Hovell) and MM-ICT
- regular checks are made at least fortnightly by Damian Fearon (IT Lead) to ensure filtering is still active and functioning everywhere. These are evidenced by reports which are reviewed and reported to SLT.
- an annual review of online safety is carried out as part of the school's safeguarding audit to ensure a whole school approach
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Sacred Heart, we expect staff to supervise children closely when using the internet. Weekly reports of web access are provided to the IT Lead who monitors and follows up on any inappropriate use.

Pupils at this school communicate with each other and with staff using Google Classroom. This is monitored closely by class teachers, SLT and the school's IT Lead.

Staff at this school use the email system provided by LGfL for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Any systems above are centrally managed and administered by the school or authorised IT partner (ie they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the Headteacher and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website This policy will also be shared with parents.
Online safety will also be covered during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

Cyberbullying (Also in Anti-Bullying Policy)

- Act as soon as an incident has been reported or identified.
- Provide appropriate support for the person who has been cyberbullied and work with the person who has carried out the bullying to ensure that it does not happen again.
- Encourage the person being bullied to keep any evidence (screenshots) of the bullying activity to assist any investigation.
- Take all available steps where possible to identify the person responsible. This may include:
    - looking at use of the school systems;
    - identifying and interviewing possible witnesses;
    - Contacting the service provider and the police, if necessary.
- Work with the individuals and online service providers to prevent the incident from spreading and assist in removing offensive or upsetting material from circulation. This may include:
    - Support reports to a service provider to remove content if those involved are unable to be identified or if those involved refuse to or are unable to delete content.
    - Confiscating and searching pupils' electronic devices, such as mobile phones, in accordance with the law.
    - Requesting the deletion of locally-held content and content posted online if necessary.
- Inform the police if a criminal offence has been committed.
- Provide information to staff and pupils regarding steps they can take to protect themselves online. This may include:
    - advising those targeted not to retaliate or reply;
    - providing advice on blocking or removing people from contact lists;
- helping those involved to think carefully about what private information they may have in the public domain.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate

images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Personal devices including wearable technology and bring your own device BYOD in school

- **Pupils/students** Year 6 are allowed to bring a mobile phone, wearable technology (including GPS tracking devices) into school, but must hand it to the class teacher for safe-keeping during the school day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. For the rest of the school (Nursery to Year 5) children are not allowed to bring their own devices or wearable technology (including GPS tracking devices) into school.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection policy. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (eg for contractors to take photos of equipment or buildings), permission of the School Business Manager should be sought and this should be done in the presence of a member staff.

- **Parents** are asked to leave their phones in their pockets and turned off when they are in school. They should ask permission before taking any photos, eg of displays in corridors or classrooms, and avoid capturing other children.

How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.
Volunteers will receive appropriate training and updates, if applicable.

Information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using the MyConcern system. The IT Lead monitors the school's reports of web filtering concerns and will take action to block harmful and inappropriate content where necessary.

This policy will be reviewed every 2 years by the Headteacher. At every review, the policy will be shared with the governing board.

Links with other policies

This Online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Behaviour Policy
- Anti-Bullying Policy
- Social Media Policy
- Complaints procedure