

Sacred Heart
Catholic Primary School



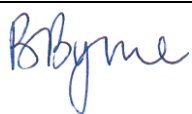
Learning in Love

E-Safety Policy

Academic Year 2020 to 2022

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	16/09/2020
Chair's Signature	
Staff Member Responsible for Review	Headteacher
Date for Review	16/09/2022

Contents

1. Aims
2. Legislation and Guidance
3. Roles and Responsibilities
4. Educating Pupils about E-Safety
5. Educating parents about E-Safety
6. Cyber Bullying
7. Acceptable use of the internet in school
8. Mobile Devices
9. Remote working and education
10. Responding to Issues of Misuse
11. Training
12. Monitoring

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

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its 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.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 ICT systems and the internet

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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 (see appendix 2) 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 e-safety in school to the Governing Body

This list is not intended to be exhaustive.

The School Business Manager (SBM)

The SBM is responsible for:

- Ensuring that appropriate filtering and monitoring systems are in place.
- 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
- Conducting a full security check and monitoring the school's IT systems on a monthly basis
- 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 any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

The IT Lead

The IT Lead is responsible for:

- 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 ICT 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: www.childnet.com/resources

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

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.

Acceptable use of the internet in school

The Social Media Policy includes information relevant to this section and also the Acceptable Use Agreements for all adults and pupils.

Pupils using mobile devices in school

Pupils in Y6 may bring a mobile phone into school, but must hand it to the class teacher for safe keeping during the school day. The schools safeguarding policy refers further to the use of mobile phone use.

Remote working and education

Staff - Staff have encrypted usb sticks to enable the secure transfer of school files to and from school. This is referred to in the schools 'acceptable use policy'. Some staff will be set up with remote access to the school's servers via a secure link and OTP device. This allows a direct log into the school network and incorporates all the school security protocols.

Pupils - LGFL school platforms are available to pupils for education and Google Classroom is being used to support pupils through learning remotely in particular online completion of some homework. Both systems are accessed securely via personal log ins. Access and documents & work uploaded are monitored regularly. The school also subscribes to externally managed systems such as tapestry and TT Rockstars to support education of pupils. All have a GDPR

assessment done on them to ensure E Safety, Data protection and security before subscribing. Access is via personal log ins.

Face to Face meetings – The school uses Zoom, Google Meet and Microsoft Teams to enable face to face meetings with parents and pupils where appropriate such as for ‘parent evenings’. Meetings require the parent to be present with the pupil and another teacher to be present with the class teacher. What is discussed can then be verified.

Further information regarding online safety can be found in the schools safeguarding policy and acceptable use agreement.

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 Safeguarding system and/or behaviour logs.

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 E-safety policy is linked to our:

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