Online Safety Policy

2022-2023

SACRED HEART CATHOLIC HIGH SCHOOL

Date reviewed: September 2022
Next Review: September 2023

Contents

1. 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.

3. Roles and responsibilities

3.1 The Local Governing Committee (LGC)

The LGC has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body safeguarding link will co-ordinate regular meetings with the designated safeguarding lead (DSL) 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 (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and to the governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT 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 ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 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 (appendix 1)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 (appendix 3).

4. Educating pupils about online safety

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

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. 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.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of Progress/Deputy Head of Progress for their child's Year Group.

Concerns or queries about this policy can be raised with any member of staff

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff will have opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health, citizenship and economic (PSHCE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 & 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Mobile phones are allowed to be brought to school by our students, although we recommend that they are not. Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

• A student's phone must be switched off and kept in their inside pocket zipped up at all times (not front pocket), unless a member of staff has given an instruction to do otherwise.

• Students are not allowed to use any phone during the School day (e.g. texting, photography, internet usage) unless a member of staff has given permission.

• A teacher may, for learning purposes, allow the students to use their phones for a specific reason (photography, accessing internet, using apps). The students will be given clear instructions to follow in these instances.

• A student is not allowed to contact anyone via phone call, text, social networking or email during the School day. This includes Parents/Guardians. Students may contact Parents/Guardians, in the case of an emergency, by using a phone in the School Office.

• Parents/Guardians are also not allowed to contact their child on a mobile device during the School day. Any message during the School day needs to go through the School Office.

• Breaches of these rules will lead to confiscation* of the phone.

The confiscated phone will be returned the student **in reception at 3.25 pm at the end of the School day on the following Friday** (if confiscated on a **Thursday or Friday, it will be returned to the student at 3.25pm in reception on the following Monday**). It will be logged and kept in a safe until this time.

• In certain lessons (e.g. PE & Technology) it is the responsibility of the student to store their mobile phone in the safe area provided by the teacher.

•When a student has their mobile phone confiscated, School will (if needed), allow the student to contact home on the Schools phone system and explain that their phone has been confiscated and will be returned to the student on the appropriate day.

Personal music systems

Personal music systems, of any type, must not be listened to during the School day, unless directed by a member of staff. Headphones must not be worn at any time. Any student seen to be wearing headphones will have the device confiscated and returned to the student at the end of the day.

Photography and Video and other electronic devices

Students are forbidden to use photography or video unless directed to by a member of staff. 'Smart watches' (e.g. Apple watch) are not allowed in school. Recording or taking pictures of a member of staff or another student by a student without permission will be taken extremely seriously and depending on the circumstances may result in permanent exclusion.

*These confiscations are allowed under governmental advice ref:

https://www.gov.uk/government/publications/searching-screening-and-confiscation

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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 (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL and Pastoral Staff log behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Student acceptable use agreement (Signed in the student planner by students and parents)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of student:

School Network

- Students must not disclose any password or login name they have been given, to anyone.
- Students must treat the ICT rooms with respect, and in no way damage equipment or fixtures and fittings.
- Students must not run or act in an irresponsible way in the ICT rooms.
- Students must not enter an ICT room without a member of staff being present.
- Students may only use the ICT rooms outside lesson times under staff supervision.
- Students should not use the network in such a way that would disrupt the use of the network by other users.
- Students must not maliciously attempt to harm or destroy data of another user.

Internet

- Students may use the Internet only as directed by a member of staff to further curriculum aims and objectives.
- Students may not enter sites for purely recreational purposes.
- Students may not use any of the mobile phone text messaging web sites.
- Should any student inadvertently access an Internet site of an inappropriate nature, she must immediately exit the site and inform a member of staff.
- Students must not download, use or upload any material, which is copyright.
- Under no circumstances should students view, upload or download any material which is likely to be unsuitable for students or schools. This applies to any material of a violent (e.g. promoting radicalisation or terrorism), dangerous, racist, or inappropriate sexual content.
- If an Internet resource is of a questionable nature, the burden of responsibility lies with the student to check with the ICT department to determine if the student should or should not access that resource, and the ICT department staff member's decision shall be final.
- Use of chat rooms is strictly prohibited.
- Students may not purchase/order items or services using the Internet at school.

School Network

- Students may only use their personal email address supplied by Sacred Heart Catholic High School when using the school's computers to communicate electronically.
- Students must not contact anyone via email unless under the direction of a member of staff.
- Students must be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is strictly prohibited. They must not state anything which could be interpreted as libel.
- Students must not contact people outside of school whom they have contacted via email at school.
- Students must not email photographs of themselves or anyone else unless permission has been given by the ICT Manager and the parent/guardian of the person it concerns.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
• Students must not give out personal details, such as telephone numbers or addresses. • Students should only open emails from sources known to them. • Note that electronic mail (email) is not private. System operators have access to all mail. **Failure to comply with these rules will result in one or more of the following:** • A sanction placed upon the student in accordance with the school behaviour policy. • A ban, temporary or permanent, on the use of the network facilities at school. • A letter informing the students' parents of the nature and breach of rules.	
Signed (pupil):	Date:
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers). *Full policy in SharePoint / Policies / IT Acceptable Use*

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:
• I will only use the IT systems at Sacred Heart Catholic High School for professional purposes
• I will ensure that all sensitive data is stored only on systems within Sacred Heart Catholic High School, or the Office 365 secure cloud storage system.
• I will ensure any personal digital devices used by me do not contain sensitive data relating to students or staff of Sacred Heart Catholic High School
• I will ensure any personal devices used in school have adequate antivirus/spyware software installed to prevent infecting school-based equipment via the network
• I agree that any sensitive data I may need to use for professional purposes while away from Sacred Heart Catholic High School will be adequately protected using encryption methods and/or password protection
• I agree to use a secure password to access the IT systems at Sacred Heart Catholic High School, and to change this every 90 days
• I will be responsible for the safety and care of any IT equipment loaned to me by Sacred Heart Catholic High School, and the security of any data stored on it
• I will lock all desktop / laptop devices while away for short periods
• I will log off all desktop / laptop devices while away for longer periods, or when another member of staff may need to log on
• I will shut down all desktop / laptop devices at the end of the day
• I will take all reasonable steps to ensure any personal digital devices which connect to the IT systems at Sacred Heart Catholic High School are protected again malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors)
• I will not use the IT systems at Sacred Heart Catholic High School for the activities stated below:
  ○ All illegal activities, and activities that contravene data protection regulations.
  ○ All activities detrimental to the success of Sacred Heart Catholic High School as well as defamation of the school.
  ○ All activities for personal benefit only that have a negative impact on the day-to-day functioning of the school.
  ○ All activities that are inappropriate for Sacred Heart Catholic High School to be associated with and/or are detrimental to the schools' reputation.
  ○ Any activity which would circumvent the IT security systems and protocols which Sacred Heart Catholic High School has put in place.	

Signed (staff member/governor/volunteer/visitor):	**Date:**