Online - Safety Policy

Governors' Review Body: Curriculum

Responsibility: Curriculum Lead

Reviewed: June 2026

Next Review Date: June 2028

Rationale

The Internet can offer many positive educational and social benefits to young people, but unfortunately there are associated dangers. Children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly. At Sacred Heart School we value highly the rich range of resources and experiences that the Internet, AI, and other technologies, can offer, to both our staff and pupils.

Aim

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

Objectives:

- To ensure that an effective range of technological tools are in place to safeguard both pupils and the system itself.
- To ensure there are clear policies, and approval processes, regarding the content that can be loaded onto the school's website.
- To educate pupils in acceptable behaviours when using the Internet and other related technologies e.g. mobile phones, chat rooms, games consoles and e- mail both in school and at home.
- To ensure all pupils, and staff, are aware of procedures they should follow if they come across anything that is offensive or worrying.
- To ensure all pupils are aware of sanctions that are in place if school policy is broken.
- To educate staff in acceptable behaviours when using the Internet and other related technologies when in school.
- To incorporate the teaching of appropriate Internet behaviour (E-safety)
- To encourage pupils to use their Microsoft Teams e-mail accounts, as opposed to other accounts, as this system is secure and monitored.
- To adopt safe practices regarding the publication of images and names of pupils on the school website. (School Consent Form)
- To ensure that the school is not infringing the intellectual property rights of others, through any publications on the school website.
- To educate staff in the use of AI within the school and its continuous development.

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 and cyber-bullying: advice for Headteachers and school staff
- 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.
The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Headteacher will report any online safety issues which have been logged within the termly report to governors

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's IT 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.
- Ensuring that any incidents of cyber-bullying are logged 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 governing board

The IT manager

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which 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 termly 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 1) 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

All staff

All staff, including agency staff 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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendices 2,3 and 4)
- To ensure that any online safety incidents are logged (see appendix 1) 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

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- 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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody
- CEOP ThinkUknow programmes

Pupils

Pupils must:

- Respect all equipment, hardware and software.
- Keep their email usernames and passwords safe, and secret, and are not permitted to use anyone else's usernames and passwords.
- Be aware of, and follow, the safe use of technology guidelines taught throughout the school.
- Be aware of the sanctions that are in place if these guidelines are not followed.
- Report any incidents of misuse within the school to a member of the teaching staff.
- Report any incidents of misuse outside of school to a trusted adult.
- Seek help/advice from a teacher, or trusted adult, if they experience problems when online; or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicate with their parent(s)/carer(s) about internet safety issues and follow school guidelines for the use of the internet, and other related technologies, at home.
- Any accidental access to inappropriate, or banned content, must be reported to a member of school staff.
- Be aware of their social responsibilities with regard to using the internet and other related technologies.
- Use AI appropriately and when under the supervision of an adult.

Pupils must not:

- E-mail malicious messages, attachments, images, or web-links to other pupils.
- Bring any form of handheld device into school e.g. mobile phones, iPads, games console etc. (Year 6 pupils may bring a mobile phone to school, with parental permission; not a Smart phone).
- Try to access inappropriate material of any sort (including pornographic, racial hatred, religious hatred, or any material not related to the lesson).
- Pass on the usernames and passwords of others to a second party.

Educating pupils about online safety

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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online and how to recognise risks

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 or Weduc. 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 Headteacher and/or the DSL.

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

Cyber-bullying

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.

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.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet.

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.

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Updating 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
- 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 IT manager].

Filtering and Monitoring (see also Safeguarding Policy)

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 our policies on Behaviour and 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 IT 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/staff code of conduct. 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.

Monitoring arrangements

The Head or DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

This policy will be reviewed every two years.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policies
- Positive Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Complaints procedure
- Acceptable Use Policy

Appendix 1: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 2: Sacred Heart School acceptable use agreement (pupils and parents/carers)

To be used from September 2021

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

When I use the school's IT systems (like computers) and get onto the internet in school I will:
1. Ask a teacher or adult if I can do so before using them
2. Only use websites that a teacher or adult has told me or allowed me to use
3. Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
4. Use school computers for school work only
5. I will be kind to others and not upset or be rude to them
6. Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly
7. Only use the username and password I have been given
8. Try my hardest to remember my username and password
9. Never share my password with anyone, including my friends.
10. Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
11. Save my work on the school network
12. Check with my teacher before I print anything
13. Log off or shut down a computer when I have finished using it
14. I will not access any inappropriate websites including: social networking sites and chat rooms or access any other inappropriate material
15. For pupils in Year 6 mobile phones will be handed in to the school each morning
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement for governors and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of governor /visitor:	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: 1. Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) 2. Use them in any way which could harm the school's reputation 3. Access social networking sites or chat rooms 4. Use any improper language when communicating online, including in emails or other messaging services 5. Install any unauthorised software, or connect unauthorised hardware or devices to the school's network 6. Share my password with others or log in to the school's network using someone else's details 7. Take photographs of pupils without checking with teachers first 8. Share confidential information about the school, its pupils or staff, or other members of the community 9. Access, modify or share data I'm not authorised to access, modify or share 10. Promote private businesses, unless that business is directly related to the school	
11. I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. 12. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. 13. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. 14. I will let the designated safeguarding lead (DOSL) and IT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. 15. I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4:

Sacred Heart Catholic Primary School

Staff Acceptable Use Policy

School networked resources, including the Primary Site School Website, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the network that would bring the name of the school, Local Authority or Diocese into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

This agreement should be read in conjunction with the following policies:

- **General Data Protection Policy**
- **ICT Policy**
- **Mobile Technology policy**
- **Disciplinary Policy**

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Staff have the responsibility to protect personal data of pupils, staff and service providers in accordance with the GDPR policy. Users will accept personal responsibility for reporting any misuse of the network or data breaches to the Headteacher.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos.

1. I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school into disrepute.

2. I will use appropriate language. I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

4. I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

5. Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.

6. I will not trespass into other users' files or folders.

7. I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.

8. I will ensure that my computer is locked if unattended for any time.

9. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact the Network Manager.

10. I will ensure that I log off after my network session has finished.

11. If I find an unattended machine logged on under other users username I will not continue using the machine – I will log it off immediately.

12. I will not use personal digital cameras or camera phones for creating or transferring images of children and young people. School owned digital cameras must be left in school overnight.

13. I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.

14. I will ensure that all documents sent electronically as attachments, containing personal data for individuals, will be password protected.

15. Where possible initials should be used in correspondence and reporting between staff.

16. I will not use the network in any way that would disrupt use of the network by others.

17. I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Network Manager.

18. I will not use "USB drives", portable hard-drives, or personal laptops on the network without having them "approved" by the school and checked for viruses. All pupil information may only be saved on 'encrypted' USB drives.

19. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

20. I will not download any unapproved software, system utilities or resources from the internet that might compromise the network or are not adequately licensed.

21. I will not accept invitations from children and you ng people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine

22. I will not place any information or postings regarding my activities at school, or the school in general on my social networking site(s). I will ensure my security settings on social networking sites are safe from unauthorised persons.

23. I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.

24. I will support and promote the school's e-safety and Data Security policies and help students be safe and responsible in their use of the internet and related technologies.

25. I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data.

26. I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.

27. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

28. I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

29. I will ensure that any Persona l Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

30. I will ensure that my ICT equipment will have the highest security settings and antivirus software.

ADDITIONAL REFERENCES

Staff must read and comply with the school e-safety policy.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is a t your own risk.

NETWORK SECURITY

Users are expected to inform the Network Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the Network Manager. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc.) if written parental consent has been given.

Please complete this form and return it to the Headteacher

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the e safety policy. If I am in any doubt I will consult the Headteacher.

- I agree to report any misuse of the network to Headteacher.

- I also agree to report any websites that are available on the school Internet that contain inappropriate material to the Network Manager.

- I agree to request permission to remove items for use at home such as laptops/IPad for the purpose of work, and will complete the relevant paperwork.

- Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher.

- If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action, I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

- I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Staff Name: _____

Staff Signature:_____ Date: _____

Appendix 5 : Sacred Heart Internet Safety Curriculum

	Curriculum content – covered each half term
EYFS	*Using Twinkl* • Buddy the Dog's Internet Safety Story • Keeping things safe
Y1	*Using Twinkl / Think you know resources.* • Owning Your Creative Work • Safe Image Searching • Staying SMART Online • My Personal Information • What is Email? • Keeping Zibb Safe Online
Y2	*Using Twinkl / Think you know resources.* • Digital footprints. • Keywords • You Be The Judge • Rate and Review • Being Kind Online • Cyber Snakes and Ladders
Y3	• What is Cyberbullying? • To Buy or Not to Buy? • Keep it to Yourself! • Emailing • Online Communication • Party Planners
Y4	• Cyberbullying • Super Searchers • Copycats! • Too Much Information? • The Online Community • Cyber Superheroes
Y5	• Spam! • Sites to Cite • Power Passwords • False Photography • Online Safety Story Planning • Online Safety Comics
Y6	• Cyberbullying • Secure Websites • People Online • Girls and Boys Online • SMARTbots • Online Safety