# SACRED HEART HIGH SCHOOL

# ONLINE SAFETY POLICY

## NOVEMBER 2025

*To be reviewed November 2026*

*This Policy should be read in conjunction with all other Sacred Heart High School Policies*

# 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 Four 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 2025, and the advice and materials it references or signposts for schools, including:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Education for a Connected World
- DfE 'Generative artificial intelligence in education'
- DfE 'Filtering and monitoring standards for schools and colleges' (current version)
- DfE 'Harmful online challenges and online hoaxes' (current version)

It also refers to the DfE's guidance on Protecting Children from Radicalisation.

This policy reflects existing legislation, including but not limited to:

- The Education Act 1996 (as amended)
- The Education and Inspections Act 2006

- The Equality Act 2010
- The Education Act 2011, which gives teachers powers to tackle cyber-bullying by, where 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 Online Safety Act 2023 (updated 2025), which strengthens duties on schools and online service providers to protect children from harmful and illegal online content
- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which set out principles for processing personal data and protecting individuals' privacy

The policy also takes into account the **National Curriculum computing programmes of study**, which include requirements for teaching pupils how to use technology safely and responsibly.

This policy complies with our **funding agreement** and **articles of association**.

## 3 ROLES AND RESPONSIBILITIES

### 3.1 The governing board

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).

The governor who oversees online safety is Patrick Sadd.

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 (**Appendices 1 & 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 deputies 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 (see **Appendix 4**) and dealt with appropriately in line with this policy
- 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 (**Appendix 3** contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or 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 [weekly/fortnightly/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.

### 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 (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

- 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 (appendices 1 and 2)

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 2**).

## 4 EDUCATING PUPILS ABOUT ONLINE SAFETY

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

Internet safety day in February is observed by school and implemented in to PSHE lessons.

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

**All** schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

### 4.1 Key Stage 3

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

### 4.2 Key Stage 4

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

By the end of Key Stage 4, pupils will know:

- 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 including a monthly newsletter, information via our website or Google Classroom. 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 and/or the DSL.

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

## 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 behaviour 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. Form teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) 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
- The school's COVID-19 risk assessment

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

### 6.4 Artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

There is the potential for pupils to misuse AI. A pupil who submits work using AI may be deemed to have committed malpractice. If the submitted work was generated solely by using AI without any reference to this fact, it is considered within the guidance of the Joint Council for Qualifications (JCQ).

The JCQ guidance on 'Any use of AI that prevents students from independently demonstrating their own attainment is likely to be considered malpractice.'

## 7 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 ICT systems and the internet (appendices 1-3). 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, 2 and 3.

## 8 PUPILS USING MOBILE DEVICES IN SCHOOL

**Mobile Phones**

All pupils are allowed to bring their mobile phone to school.

A yonder pouch has been provided for pupils in Year 7-11. During form time, pupils in these years must secure their phones in the pouches, which are then unlocked at the end of the day upon exiting the school building.

Sixth formers are permitted to have their mobile phones in school, but usage is limited to designated times and areas specified in the parent handbook.

Limits on use as outlined in the school's behaviour policy. Any use of mobile devices in school must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy.

**Other mobile devices with internet access**

Other mobile devices with internet access (such as ipads or Apple smart watch) are not allowed in school for any year group.

## 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 2**.

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.

## 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 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 Policy. 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, 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 deputies 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 logs behaviour and safeguarding issues related to online safety. An incident report log can be found in **Appendix 4**.

This policy will be reviewed every year by the Associate 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:

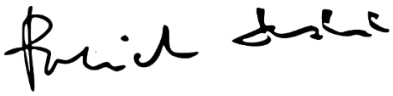
- Child Protection and Safeguarding Policy
- Learning and Living (Behaviour) Policy
- Staff Disciplinary Policy & Procedures
- Data Protection Policy and Privacy Notices
- Complaints Policy
- Acceptable Use Policies

## 14 RATIFICATION

This Online Safety Policy builds on best practice and government guidance.

The Policy has been approved and ratified by the Headteacher and the Ethos Committee of the Governing Body in November 2025.

Mrs S O'Donovan
Headteacher



Patrick Sadd
Chair of Ethos Committee

# Appendix 1

# STUDENT COMPUTER RESOURCES POLICY & ACCEPTABLE USE AGREEMENT

*This agreement will keep everyone safe and help us to be fair to others.*

The school has provided computers for use by pupils in school and in some occasions, at home, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all pupils, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

## POLICY

**Equipment**

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will result in access being withdrawn.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software, and ensure they have been found to be clean of viruses, before connecting them to the network.
- Protect the computers from spillages by not eating or drinking whilst using the ICT equipment.

**Security and Privacy**

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Never share personal information via the internet like your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas will be treated like school lockers. Staff may review your files and communications to ensure that you are using the system responsibly.

**Internet**

- You should access the Internet only for study or for school authorised/supervised activities.

- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- If you are unhappy or have any doubts about any communication/contact via the internet please inform a member of staff immediately.

**Email**

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

**Social Media**

- Do not do anything that could be considered discriminatory against, or bullying or harassment of, any individual e.g. making offensive or derogatory comments relating to sex, gender reassignment, race, disability, sexual orientation, religion or belief or age; using social media to bully another individual or; posting images that are discriminatory/offensive or links to such content.
- Breach copyright e.g. using someone else's work, such as images or content without permission; failing to give acknowledgement where permission has been given to reproduce something;

**Cyber bullying**

The school is strongly committed to equality, diversity and inclusion and has zero tolerance to any forms of harassment and discrimination by students, members of staff, or other members of the school community.

The following examples illustrate the types of behaviour, displayed through social media communications, which the school considers to be forms of cyber bullying:

- Maliciously spreading rumours, lies or gossip.
- Intimidating or aggressive behaviour.
- Offensive or threatening comments or content.
- Posting private images of an individual without consent (including, but not limited to, private sexual images of an individual).
- Sharing unwanted images (including sexual images).
- Posting comments, photos, etc; deliberately mocking an individual with the intent to harass or humiliate them.
- Sending messages or posting comments with the intent to trick, force or pressure the receiver into doing something that they would not otherwise be comfortable doing (grooming).

**Guidelines for AI Use**

- **Supplemental Aid**: AI can be used as a tool for assistance in brainstorming ideas, understanding complex texts, or improving grammar and syntax. However, the bulk of the thinking, analysis, and composition should be your own.

- **Reference and Citation**: If significant insights or phrases are borrowed from AI, these should be properly cited, much as you would cite a human source.
- **Clarification, Not Substitution**: Use AI for clarifying doubts or seeking explanations, not as a shortcut to avoid reading, analysis, and comprehension.
- **Learning, Not Completing**: Use AI as a tool for learning, not just for task completion. Your primary goal should be understanding and skill development, not simply finishing an assignment.
- **Tutoring, Not Completing**: Use AI to ask questions as you would your teacher. Just as your English teacher would not provide "what are the answers," neither should AI.

# ACCEPTABLE USE AGREEMENT

1) I will only use the school's computers for schoolwork, homework and as directed.
2) I will only edit or delete my own files and not view, or change, other people's files without their permission.
3) I will keep my logins, IDs and passwords secret.
4) I will use the Internet responsibly and will not visit web sites I know to be banned by the school. I am also aware that during lessons I should visit web sites that are appropriate for my studies.
5) I will never use mobile devices, websites or social networking sites such as Facebook to make derogatory comments about the school, staff or other pupils
6) I will only e-mail people I know, or those approved by my teachers.
7) The messages I send, or information I upload, will always be polite and sensible.
8) I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
9) I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
10) I will never upload images of others onto a computer, mobile device or social networking site or pass on images of others without their permission
11) I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
12) If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
13) I am aware that some websites and social networks have age restrictions and I should respect this.
14) I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
15) I am aware that all my activities on the computer are constantly monitored for my own safety and can be used against me if I breach school policy.
16) If I misuse the IT facilities in a way that breaches school policy, including the behaviour policy, I understand that the school will take action which could lead to having access to the IT facilities being taken away and/or to exclusion.

17) I agree that all IT resources available to me from the school shall be used in a sensible manner which in no way is disruptive or abusive. This refers to both hardware and software.

**Please read the Computer Resource Guidelines and Acceptable Use commitments carefully.**

Only once these have been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with the existing policy regarding school behaviour. For serious violations, action will be taken in line with the school's discipline policy. Where appropriate, police may be involved or other legal action taken.

*I have read and understood the above and I agree to use the school computer facilities within these guidelines and to abide by the Acceptable Use commitments in this agreement.*

**Student Name:**

**Signature:**

*I have read and understood the above.*

**Parent/Guardian Name:**

**Signature:**

# Appendix 2

# ACCEPTABLE USE AGREEMENT STAFF

Sacred Heart High School has provided computers for use by staff both home and at work, offering great potential to support the curriculum. The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.

**Equipment**

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the IT equipment.
- Only use the computers for educational purposes - buying or selling goods personal goods is inappropriate.
- Always check personal mobile equipment (e.g. laptops, mobile phones.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the Guest network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- Be professional in your use of I.T. equipment and systems. Set a good example to students of how to look after the schools' I.T. resources.
- Always report faults or issues to the I.T. department helpdesk as soon as possible. Do not assume that others may have already reported it.

**Security and Privacy**

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Other computer users should be respected.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas will be treated like school lockers. IT staff may review your files and communications to ensure that you are using the system responsibly.
- All data held by the school must be used in accordance with the schools' data protection policy and current data protection legislation.

**Internet**

- You should access the Internet only for school activities.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

**Email**

- Remember to always use professional email etiquette. Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

**Social Media**

- Staff must follow statutory and school safeguarding procedures at all times when using social media.
- Staff must maintain the reputation of the school, its staff, its pupils, its parents, its governors, its wider community and their employers on social media.
- Staff must not contribute or access any social media content which is illegal, discriminatory, sexual, or otherwise offensive when linked in any way to the school.
- Staff must not use social media to criticise members of the school community.
- Staff must not breach school confidentiality. You must not for example discuss children or parents on a department WhatsApp group or any matters pertaining to the school or members of its community on other social media platforms.
- Staff are responsible for the configuration and use of any personal social media accounts they have. They are responsible for determining the level of security and privacy of all their social media content. It is highly recommended to your social media profiles at a private setting, which can only be viewed by family and friends.
- The school reserves the right to monitor all staff internet use, including when staff are making personal use of social media, on any school systems or equipment. Misuse of social media – even personal use – on school equipment is a breach of the school's acceptable use policy.
- Prior to uploading content to the school's social media accounts, staff allocated to this task must sign the school's Social Media Terms of Use Agreement, which can be found in the policies folder in Sharepoint.

**Please read this document carefully. Only once it has been signed and returned will access to the School network be permitted. If you violate these provisions, access to the School network will be denied and you will be subject to disciplinary action.** Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Date:

Name:

Signature:

# Appendix 3
# Online Safety Training Needs Self-Audit for Staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

# Appendix 4: 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** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |