ST. ANNE'S CATHOLIC HIGH SCHOOL FOR GIRLS

ONLINE SAFETY POLICY

Spring 2025

Next Review: Spring 2027

Quality of Education Committee

Mission Statement

St. Anne's Catholic High School for Girls will offer a positive presence in Enfield with a comprehensive curriculum equipping students with the ability to meet the challenges of the 21st Century confidently and with high spiritual and moral standards.

We recognise that students, parents, staff and governors make up the school's community which will continually self-evaluate to improve itself effectively and efficiently in all aspects of its growth.

'Act justly, love tenderly, walk humbly with your God.'

Contents

1. Aims

Our school aims to:

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

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 and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 , 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 students' electronic devices where they believe there is a 'good reason' to do so.

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).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)

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 (DSL)

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well 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, IT manager and other staff, as necessary, to address any online safety issues or incidents and to ensure that the school has robust filtering and monitoring in place
- Ensuring that any online safety incidents are logged on MyConcern 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
- 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 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 students 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 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 5) 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 IT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendices 1)

- Working with the DSL to ensure that any online safety incidents are logged on My Concern 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
- Monitoring students' use of the internet when they are supervising them in class or around the building.

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 IT 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 factsheet - Childnet International
- Resources and guides for parents - ThinkUKnow
- Support and guidance for parents - Parentzone

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

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

In **Key Stage 3**, students 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

Students 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 secondary school**, students 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

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

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

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 https://www.st-annes.enfield.sch.uk/ or via Ms Office 365 our virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during the year 7 Information Evening. We also direct parents to relevant events run by the local authority and other agencies as appropriate.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Learning Support Coordinator or the Designated Safeguarding Lead.

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 students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes citizenship, personal, social, health and economic (CPSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, 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 students, 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 where deemed necessary.

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 students' 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 DSL or other member of the senior leadership team to decide whether they should:

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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT 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 students, 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. Students using mobile devices in school

Students are not permitted to use a mobile phone during school hours or whilst on school premises either inside the school building or in any outside area on school grounds. Students should not be using their mobile phones as they approach the school entrance, and all mobile phones should be switched off as soon as they arrive at the school gate before entering the school grounds. If a student fails to meet this expectation and is seen with a mobile phone, the device will be confiscated and stored securely in Reception and returned to the student at the end of the school day; the student will receive a Senior Mentoring and Development session. Any further incident may result in an Internal Suspension and the mobile phone confiscated pending parental/carer collection.

The only exception to this is when given explicit permission by a member of staff, for example, for teaching and learning purposes in class. In such a case the member of staff takes responsibility for supervising and monitoring the use of the device.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the staff acceptable use policy (AUP).

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour, IT 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 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 and 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.

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).

The 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 logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed at least every two years by the DSL and online safety coordinator. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Positive Behaviour for Learning Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Acceptable Use policy (AUP)
- IT and internet acceptable use policy

Modification history:

Version	Date	Description	Revision Author
0.1	Autumn 2021	Online Safety Policy	Claudia Duarte/Emmanuelle Danneau-Joyce
0.2	Autumn 2024	Online Safety Policy	Claudia Duarte/Kaylea Vevers

Appendix 1 - Student Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS

Name of student:

I will read and follow the rules in the acceptable use agreement policy. When I use the school's IT systems (like computers) and get onto the internet in school:

I will:

- Always use the school's IT systems (computers) and the internet responsibly and for educational purposes only
- Only use them when a member of staff is present, or with their permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address, telephone number or email to anyone without the permission of a member of staff or parent/carer
- Tell a member of staff(or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details

If I bring a personal mobile phone or other personal digital device into school:

- I will not use it during lessons, tutor group time, break time, lunchtime, clubs or other activities organised by the school, without a member of staff permission
- If permitted by a member of staff, I will use my mobile phone/personal digital device, responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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 (student):	**Date:**

Parent/carer's 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 students 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 2 - Acceptable Use Agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

St. Anne's is a professional organisation with a responsibility to safeguard its community. All staff are expected to use the school's IT systems in a professional, lawful, and ethical manner. This policy is designed not to restrict how staff use technology for teaching or personal purposes but to ensure safe, responsible use and protect the school's systems from misuse.

Key Expectations

- **Monitoring:**
  I understand that members of the Senior Leadership Team or IT Team may view my computer screen or online documents at any time without prior notice.
- **Privacy:**
  I am aware that work emails and files are not private. All internet and network activity can be logged and reviewed by my manager if requested.
- **Data Handling:**
  I will save, access, and delete documents according to the school's network security and confidentiality protocols.
- **Use of Technology:**
  I will use the school's digital technology and systems only for professional purposes or reasonable personal use approved by the Head and Governing Body.
- **Email Use:**
  I will use only the school's approved and secure email system (e.g., …@st-annes.enfield.sch.uk) for school business.
  I will avoid sending work emails between 6pm and 6am on weekdays, and between 6pm Friday and 6am Monday, and understand I am not obliged to respond during these times.
- **Content and Conduct:**
  I will not browse, download, or send material offensive to colleagues.
  I will report any accidental access to inappropriate material or breaches of internet filtering to the appropriate manager.
- **Access Control:**
  I will not allow unauthorized individuals to access school email, internet, intranet, network, or other Local Authority systems.
- **Device Security:**
  I will protect devices by logging out or locking screens when unattended, in the staffroom or classes, and will not leave devices visible or unsupervised in public places.
  I will not download unlicensed or potentially harmful software.
- **Passwords and Software:**
  I will keep my passwords confidential and never share them.
  I will only connect devices with up-to-date antivirus software to the school network.
- **Safeguarding and Digital Safety:**
  I will stay informed about digital safeguarding and ensure these principles are reflected in my teaching and communications.
- **Use of Cameras and Mobile Devices:**
  Any photos or videos of students taken during school events or trips must be uploaded to the school network by the Friday of the week they were taken, and must not be left on personal devices, in line with safeguarding and data protection policies.

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

- **Learning Platform and Remote Access:**
  I will use the school's Learning Platform and follow London Grid for Learning guidelines. For remote work, I will use school devices or connect via the school VPN when using personal devices.

Data Protection and Confidentiality

- I will not email any student data or confidential information to personal email accounts to comply with GDPR and Safeguarding.
- Student images stored on personal devices must be deleted every Friday from all folders, including camera and downloads folders.
- I acknowledge the importance of separating my personal and professional digital lives to protect sensitive information.

Professional Boundaries Online

- I will ensure personal social media or blogs are clearly separate from my professional role.
- I will avoid any online activity that could compromise my professional responsibilities.

Use of School Equipment

- Any computer or device loaned by the school is for professional use only.
- I will notify the school of any significant personal use of school devices, as defined by HM Revenue & Customs.

Confidentiality and Legal Obligations

- I will keep all staff and student information confidential unless legally required to disclose it to an appropriate authority.

Compliance

- I agree to follow this policy and understand that failure to comply may result in disciplinary action.

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