St Augustine's Catholic High School and Sixth Form

E-Safety Policy

Approved		**Date**
Principal G T O'Connor		08.09.21
Cycle of Review:	**3 years**	
Next Review Date:	**June 2024**	

ST AUGUSTINE'S CATHOLIC HIGH SCHOOL AND SIXTH FORM

DEVELOPING THE WHOLE PERSON

E-SAFETY POLICY

Our school aims are to:

- Have robust processes in place to ensure the online safety of pupils, parents, staff 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
- Enable students to learn creatively and effectively and encourage collaborative learning and the sharing of good practice amongst all school stakeholders.

These agreements and their implementation will promote positive behaviour, which can transfer directly into each student's adult life and prepare them for experiences and expectations beyond school. It is our aim to embed knowledge for responsible and mature online users.

Current Role Holders, as of September 2020

Assistant Principal for Pastoral Care and DSL:	Mr N Murphy
Deputy Safeguarding Lead:	Mr N Murphy, Mr N Deakin
E-Safety Co-Ordinator:	Mr N Murphy
Lourdes IT Manager:	Matthew Setchell (Lourdes IT)
Safeguarding Governor:	Mrs C Hubble

1. Our Vision

Saint Augustine's Catholic High School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable dangers and risks. We aim to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

E-Safety Policy Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned and used by adults and young people while on the school premises.

Promotion of E-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible Internet users. To achieve this, we will:

- Make this policy and related documents available on the school website at: https://www.sta.magnificat.org.uk/
- Introduce this policy and related documents to all stakeholders at appropriate times. This will be at least once a year and after updates.
- Post relevant e-Safety information in all areas where computers are used.
- Provide e-Safety information and support for parents during parent evenings, community workshops and through the school bulletin.

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 Principals and school staff
- 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 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. This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Principal 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 Cecilia Hubble. All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1)

The Principal

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

The Designated Safeguarding Lead

Details of the school's DSL and deputy/deputies are set out in our child protection and safeguarding policy including relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, deputy safeguard lead, e-Safety coordinator, Lourdes IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see Appendix 3) 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 2 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 Principal and/or governing board
  This list is not intended to be exhaustive.

The Lourdes IT Manager
The Lourdes 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 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 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 3) and dealt with appropriately in line with this policy
  This list is not intended to be exhaustive.

All Staff
All staff, including contractors and 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 ICT systems and the internet (Appendix 1), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 3) 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.

Parents
Parents are expected to:

- Notify a member of staff or the Principal 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 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

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 1).

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. The text below is taken from the National Curriculum computing programmes of study.

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- 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
- The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and form time activities to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils 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. This policy will also be shared with parents. Online safety will also be covered during parents' evenings and through community workshops. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. 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 (see also the school behaviour policy.) The school has a zero tolerance approach on cyber-bullying. We take all incidents very seriously and will complete a full investigation to establish the surroundings of the alleged incident and will respond appropriately to all parties involved.

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. Subject teachers/form 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 personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff and governors (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. 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.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet

All pupils, parents, staff and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1 and Student Acceptable Use Policy). 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, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in Appendix 1 and Student Acceptable Use Policy.

8. Pupils using Mobile Devices in School

Pupils may bring mobile devices into school, but they are to be placed and locked in the Yondr pouch, provided by the school. Students are not allowed to unlock the pouch during the school day unless given consent by their teacher. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a pupil 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 Appendix 1. 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 Lourdes IT Manager. Work devices must be used solely for work activities.

10. Physical Environment/Security

Environment Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system, consulting with the Local Authority where appropriate.

- Central filtering is provided and managed by Worcester County Council. All staff and students understand that if an inappropriate site is discovered it must be reported to the Lourdes IT Manager who will block the site through Smoothwall. All incidents will be recorded through an incident report on SIMS for audit purposes.
- The school uses Policy Central on all school owned equipment to ensure compliance with the Acceptable Use Policies.
- Students use is monitored by the Lourdes IT Manager (Lourdes IT).
- Staff use is monitored by the Lourdes IT Manager and passed to the Principal.
- All staff are issued with their own username and password for network access. Visitors / supply staff are issued with temporary usernames and passwords and the details recorded in the ICT Services Helpdesk.
- All students are issued with their own username and password and understand that this must not be shared.

Email

The school email system is provided, filtered and monitored by Worcestershire County Council filtering and is governed by Worcestershire City Council Email Use Policy. I thought that as an academy, then Lourdes IT were responsible for the school email system.

- Both staff and students are given a school email address that can be used for professional and educational purposes
- Working with the Principal, deputy safeguard lead, e-Safety coordinator, Lourdes IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see Appendix 3) 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 2 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 Principal and/or governing board Everyone in the school community understands that the email system is monitored and should not be considered private communication.
- Guidance is given to the school community around how email should be structured when using school email addresses

- Staff are allowed to access personal email accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the email policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Students may be given the opportunity to check their own email outside directed time and understand that any messages sent using the school equipment should be in line with the email policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate emails must be reported to the class teacher / e-Safety coordinator as soon as possible.

Published Content
The Principal takes responsibility for content published on the school website. The school will hold the copyright for any material published on the school website or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

- The school encourages the use of email to contact the school via the school office / generic email addresses / staff email addresses
- The school does not publish any contact details for the students
- The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school website or creates a school account on the site

Digital Media
We respect the privacy of the school community and will obtain written permission from staff, parents, carers or students before any images or video are published or distributed outside the school.

- Photographs will be published in line with Government guidance (www.education.gov.uk) and not identify any individual student.
- Students' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to students taking part in external video conferencing.
- Students understand that they must have their teacher's permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the students

Social Networking and Online Communication (see Social Media Policy)
The School has chosen to restrict the use of some social networking sites and online communication including Facebook and Instagram. Students' understand that they need their teacher's permission to access these sites using their own equipment and whilst on school property. Guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Students are given age appropriate advice and guidance around the use of such sites.

Educational Use
School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material.

- Where appropriate, links to specific websites will be provided instead of open searching for information.
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind students of the Acceptable Use Polices before any activity.
- Staff and students will be expected to reference all third-party resources that are used

Data Security and Protection
Personal data will be recorded, processed, transferred and made available in line with General Data Protection Regulation (GDPR).

11. 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 related policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/Staff Code of Conduct 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.

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

13. Monitoring Arrangements
The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 3. This policy will be reviewed annually or when an update occurs by the e-Safety Coordinator. At every review, the policy will be shared with the governing board.

14. Links with Other Policies
This online safety policy is linked to our:
- Child protection and safeguarding policy
- Peer to peer abuse policy
- Acceptable Use Policy for Staff
- Acceptable Use Policy for Students
- Social Media Policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Acceptable Use Agreement for Staff, Governors and Visitors

Name of staff member/governor/visitor: _____

This document forms part of the school's Safeguarding Policy, e-Safety Policy and Social Media Policy. All employees and visitors to the school should sign the appropriate section to show that they have read, understood and agree to the rules included. The full policies are available on the school website.

The term 'Internet' in this policy includes the use of social media platforms.

The purpose of this policy is to safeguard and protect all members of the school community online.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- 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)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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.

I agree that the school will monitor the websites and social media platforms I visit and my use of the school's ICT facilities and systems.

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.

I will let the designated safeguarding lead (DSL) deputy/deputies 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.

I will always use the school's ICT systems and the internet responsibly and ensure that pupils in my care do so too.

Signed (staff, governors, visitor): _____

Date: _____

Appendix 2

Online Safety Training Needs – Self Audit for Staff

Name of staff member/governor/visitor: _____

Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
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, 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 3

Online Safety Incident Report Log

Date	Where the incident occurred	Description of the incident	Action taken	Name and signature of staff member recording the incident