St Augustine's Catholic High School and Sixth Form

Social Media Policy

Approved		**Date**
Principal G T O'Connor		01.07.20
Cycle of Review:	**3 years**	
Next Review Date:	**June 2023**	

ST AUGUSTINE'S CATHOLIC HIGH SCHOOL AND SIXTH FORM

DEVELOPING THE WHOLE PERSON

SOCIAL MEDIA POLICY

Our school aims are to:

- Safeguard and protect all members of the school community online
- Identify and implement approaches to educate and raise awareness on the use of social media and online safety
- Enable all employees and students to work safely and responsibly, to role model positive behaviour online and to manage professional standard and practice when using social media platforms
- Enable students to learn creatively and effectively and encourage collaborative learning and the sharing of good practice throughout the school community
- Embed knowledge for responsible and mature use of social media that will benefit our students beyond school
- Deliver an effective approach in the use of social media, which empowers us to protect and educate the whole school community
- Identify clear procedures to use when responding to social media concerns

Current Role Holders, as of September 2020

Assistant Principal for Pastoral Care and DSL:	Mr P Foley
Deputy Safeguarding Lead:	Miss C Bird
E-Safety Co-Ordinator:	Ms J Walkley
Lourdes IT Manager:	Matthew Setchell (Lourdes IT)
Safeguarding Governor:	Mrs C Hubble

1. **Introduction**

Social media is the term used for internet-based tools used on digital devices to help people keep in touch and enable them to interact in order to share information, ideas and views. Whilst St Augustine's Catholic High School and Sixth Form recognises and embraces the numerous benefits and opportunities that social media offers, it is crucial that employees, parents/carers and students are aware that there are some associated risks, especially around the issues of safeguarding, bullying, cyber bullying and personal reputation.

Websites and applications dedicated to forums, blogging/vlogging, social networking, social bookmarking, social curation and wikis are among the different types of social media. This policy

applies to the use of all forms of social media. It applies to use of social media for professional purposes as well as personal use that may affect the school in any way.
St Augustine's Catholic High School and Sixth Form already utilises a number of communication channels, e.g. school website, twitter feeds, Facebook, text messaging systems, notice boards, bulletins etc. and recognises the importance that these play in ensuring effective communication. As technology advances and social media dominates our communication tools, it is impossible to cover all circumstances of emerging media, but the principles set out in this policy must be followed irrespective of the medium used.

It is recognised that stakeholders of the school will have their own personal social media accounts. Personal accounts should not be used for professional communication. All school stakeholders have a duty of care and therefore are expected to adopt high standards of behaviour, they should maintain appropriate boundaries and manage personal information effectively to avoid misuse.

2. Our Vision

Saint Augustine's Catholic High School embraces the positive impact and educational benefits that can be achieved through appropriate use of social media 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.

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 Social Media

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.
- 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 information in all areas where social media platforms are used.
- Provide information regarding the use of social media and support for parents during parent evenings, community workshops and through the school bulletin.

3. Legislation and Guidance

All stakeholders are bound by a legal duty of care and other laws to protect confidential information they have access to in their professional role. Disclosure of confidential information on social media platforms is likely to be a breach of a number of laws and professional codes of conduct including GDPR. Other laws relating to libel, defamation, harassment, copyright and intellectual property may also apply.

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

4. 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 social media 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 incidents regarding the use of social media are logged (see Appendix 3) and dealt with appropriately in line with this policy
  This list is not intended to be exhaustive.

5. Acceptable Use

Expectations

The expectations' regarding safe and responsible use of social media applies to all stakeholders of St Augustine's Catholic High School and Sixth Form.

- All stakeholders of the school are expected to engage in social media in a positive, safe and responsible manner
- Stakeholders are advised not to publish personal opinions, concerns, pictures or messages on any social media platform used as a professional communication tool, especially content that may be considered threatening, hurtful or defamatory to others
- The school will monitor the use of social media when accessed via the schools' network
- Restricted access to social media sites is in operation via the schools' network
- Concerns regarding the use of social media should be reported to the DSL, deputy/deputies or e-Safety coordinator, and will be managed in accordance with the schools related policies.

Employee expectations

- All employees are advised that their conduct on social media can have an impact on their role and reputation within the school environment.
- Disciplinary action may be taken if any actions of individuals bring the school or profession into disrepute, or if something is felt to have undermined confidence in their professional abilities/school environment.
- Safe and professional behaviour will be outlined for all employees (including visitors) as part of the induction process as is contained in other relating polices
- All stakeholders of the school are advised to safeguard themselves and their privacy when using social media platforms.
- Advice will be provided to employees via staff training and by sharing appropriate guidance and resources on a regular basis. This will include but is not limited to:
  - Setting and updating privacy levels of their personal sites
  - Being aware of location sharing services
  - Opting out of public listings on social networking sites
  - Keeping passwords safe and confidential
  - Ensuring their personal views are not deemed to be those of the school
- Employees are encouraged not to identify their school as their place of work for the following reasons:
  - Avoid unwanted friend requests
  - Ensure the safeguarding and privacy of all stakeholders
  - Prevent information on these sites from being linked to the school
- Employees are encouraged to carefully consider the information, including text and images, they share and post online and to ensure their social media use is compatible with their professional role and is accordance with policies and the wider professional legal framework.
- Information that employees have access to as part of their employment, including photos and personal information about learners and their family members of colleagues will not be shared or discussed on social media platforms.
- Employees will notify the DSL or Principal immediately if they consider that any content shared on social media platforms conflicts with their role.

Communicating with learners and parents/carers
All employees are advised not to communicate with or add as friends any current or past learners or their family members via any personal social media sits, applications or profiles except in cases where a personal relationship already exists.

  - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL or deputy/deputies and/or the Principal.
  - If ongoing contact with learners is required once they leave the school, employees should use the existing alumni networks or use the schools' official communication tools.
- Employees will not use personal social media platforms to contact learners or parents/carers, nor should any contact be accepted, except where prior authorisation has been approved by the DSL or Principal.
- Any communication from learners and parents received on a personal social media platform will be reported to the DSL or Principal.

Student expectations
All students are advised that the Acceptable Use Policy encompasses their conduct on social media whether on or off school premises should their actions implicate the school in any manner.

- Not accessing social media sites on school devices or on personal devices whilst at school.
- Not make inappropriate comments (including private messages) about the school, teachers, governors, supporting staff, other students and/or their parents/carers.
- Not posting images of themselves in school uniform or using any of the schools' logos.
- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, through assemblies and form time activities using age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning bullying, cyber bullying, sexting, use of unauthorised sites, underage use of social media sites, games or tools.

Learners will be advised to:
Consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

- Only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- Use safe passwords.
- Use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within school and externally

Parent/Carers expectations
We ask parents to fully support our commitment to safe and responsible use of social media platforms, this includes parents taking responsibility for their actions on social media and for parents to consider or refrain from the following:

- Posting images or comments that include/name other stakeholders of the school, including students and their parents/carers.
- Not use social media platforms whilst on the school premises or on a school trip/event.
- Raise queries/concerns directly with the school through the appropriate channels rather than posting on social media platforms.
- Not posting anything malicious about the school or wider community.

6. School Use of Social Media

St Augustine's Catholic High School and Sixth Form official media sites are a twitter account, Instagram account and a Facebook page. The official use of social media sites only takes place with clear educational or community engagement objectives, with specific outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Principal. SLT have access to account information and login details for our social media channels, in case of emergency, such as staff absence. Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

- Staff use email addresses provided by the school to register for and manage any official social media channels.
- Official social media sites are suitably protected and linked to our website.
- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: antibullying, image/camera use, data protection, confidentiality and child protection.

- All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving learners will be moderated possible.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

Employee Official Use of Social Media

Employees who follow and/or like our official social media channels will be advised to use dedicated professional accounts to avoid blurring professional boundaries. If employees are participating in online social media activity as part of their capacity as an employee of the school, then they will:

- Sign our social media acceptable use policy.
- Always be professional and aware that they are an ambassador for the school
- Disclose their official role but make it clear that they do not necessarily speak on behalf of the school.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection, intellectual property and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.

- Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the Principal of any concerns, such as criticism, inappropriate content or contact from learners.

7. How the School will Respond to Misuse of Social Media Platforms

Where a pupil breaches this policy, 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 breaches this policy then 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.

8. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including social media use, 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. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

9. 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.

10. Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Acceptable Use Policy for Staff
- Acceptable Use Policy for Students
- E-Safety Policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Worcester County Council Filtering Policy

Appendix 1

Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor: _____

This document forms part of the school's Safeguarding Policy, e-Safety Policy and Social Media Policy. All employees, volunteers 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, volunteer, visitor): _____

Date: _____

Appendix 2

Online Safety Training Needs – Self Audit for Staff

Name of staff member/governor/volunteer/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, 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 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