Mission Statement

Let God's love shine in our lives as we grow and learn together, living out the Gospel Values of faith, hope and love for ourselves and others.

Social Media Policy

Date reviewed:	December 2023
Date approved:	December 2023
Date due to review:	Autumn 2024

Introduction

This policy sets out St. Alban's Catholic Primary and Nursery School's policy on social networking. Social networking activities conducted online, outside of school can have a negative effect on an organisation's reputation or image. This includes, but is not limited to, blogging, involvement in any social networking sites such as Facebook, Instagram or X, and posting material, images or comments on sites such as YouTube, Online discussion forums, Collaborative spaces, Media sharing services, and 'Microblogging' applications.

In addition, St. Alban's Catholic Primary and Nursery School has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

This policy should be read in conjunction with other relevant school policies such as the Safeguarding, Equal Opportunities, Curriculum, Finance, Teaching & Learning, SEND, Data Protection, Freedom of Information, Disciplinary Procedure, and Behaviour and Anti-bullying policies.

The policy has been developed by the Computing Leader in consultation with the SENCO, Leadership Team and teachers. Guidance from experts and pupil, parent and staff voice has shaped and will continue to help shape this policy.

Context

St Alban's is an average sized Catholic Primary and Nursery School, a member of St Clare CMAT, Diocese of Hallam and works closely with the Catholic Dearne Valley Family of Schools as well as the Sheffield Catholic Schools who are part of St Clare's. Our mission as a Catholic school is to create and develop a community centred upon the teaching of Jesus Christ where all individuals are enabled to reach their full potential in all elements of their lives. Our age range is 2 to 11 with 217 on roll, 187 FTE R – Y6. St Alban's Nursery opened in September 2021, and is led by teachers and experienced qualified Early Years practitioners and has continued to grow in numbers. St Alban's serves the local parishes of St Alban's Catholic Church of Denaby and Conisbrough and Blessed English Martyrs, Mexborough all of which are in the town of Doncaster. The school is in the highest 20% of socio-economically deprived catchments in the country and is one of the 5 most deprived schools in Doncaster with a changing profile of number of Catholics attending. In recent years, there have been children with more complex needs attending and from Y4 down to our youngest learners in Nursery, 80% of children in these classes fall within the 10% most disadvantaged in the country. At St Alban's 41% children are disadvantaged and a higher than average proportion of children with SEN at 32%, most of whom have speech, language and communication (63%) and/or social, emotional and mental health (27%) needs. Children entering EYFS are doing so with increasingly signficant needs and our current Reception class have 44% of children with complex SEN. Most children at St Alban's are of White British heritage, with a lower than average proportion of children with EAL at 3.23%. St Alban's has lower than national levels of stability and since January 2021 there has been a 15% increase in the number on roll (R – Y6) therefore increasing mobility factors. Prior to COVID, attendance was 97.48% but reduced significantly with 27.8% persistently absent in 21/22 academic year. During the school year 22/23, attendance improved at a significantly higher rate than the national primary rate reaching 94.03%, an increase of 2.13% on 21/22 and a reduction to less than national levels for persistent absence at 19.6%.

Implementation and Review of Policy

Implementation of the policy will take place after consultation with the Governors in the Spring term 2024. This policy will be reviewed every year by the Head teacher, computing leader, the Governing Body and Staff. The next review date is Spring term 2025.

Dissemination

The draft policy will be given to all members of the governing body, and all teachers, teaching assistants and non-teaching members of staff. Copies of the document will be available to all parents through the school's website and a copy is available in the school office.

Key principles

- Everyone at St. Alban's Catholic Primary and Nursery School's has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
- It is important to protect everyone at St Alban's from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is paramount and is a key responsibility of all members of staff and it is essential that everyone at St Alban's School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as an employee or volunteer must not communicate with children via social networking.
- With safeguarding in mind, staff, parents and visitors are prohibited from using mobile phones in public areas around school and on school premises.
- This policy relates to social networking outside of school. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Headteacher.
- It is also completely unacceptable to communicate on social media about the school or any member of the school community in or out of work on personally owned equipment.
- The school's Online Safety Policy outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience.

Our aims:

- To set out the key principles and code of conduct expected of all members of staff, governors, Friends, volunteers and pupils at St Alban's School with respect to social networking.
- To further safeguard and protect children and staff.
- Teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. We aim to give clarity to the way in which social media/mobile phones are to be used by pupils, social media/mobile phones are to be used by pupils, governors, visitors, parent helpers, volunteers and school staff at St. Alban's Primary.
- Provide guidance for parents.

- Address the expectations in key areas:
    1. The use of social networking sites by pupils within school
    2. Use of social networking by staff in a personal capacity
    3. Comments posted by parents/carers
    4. Dealing with incidents of online bullying
    5. The use of social networking sites by pupils within school

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 head teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Overview and Expectations

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, public in general and all those with whom they work. Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting. The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with children. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them. School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

Code of Conduct: Social Networking by staff in a personal capacity

This policy deals with the use of all forms of social media including, but not limited to, Facebook, LinkedIn, Twitter, Wikipedia, and all other internet postings, including blogs.

Under no circumstances should staff make reference to any staff member, pupil, parent or school activity/event.

The following are also not considered acceptable at St Alban's School:
- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.
- In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties. All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.
- Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the school, or another school, Hallam Diocese or Doncaster City Council could result in formal action being taken against them. This includes the uploading of photographs which might put the school into disrepute.
- In addition to the above, all staff at St Alban's School must ensure that they:
  - Communicate with children and parents in an open and transparent way using the school phone number and email address.
  - Never 'friend' or 'follow' a pupil on any social networking site (including past pupils under the age of 16).
  - Staff are strongly advised not to add parents as 'friends' on their personal accounts.
  - Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
  - Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.
  - Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
  - Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
  - Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality if they choose to use social media.
  - Mobile phones must not be used on the premises by parents and carers.

Code of Conduct: Social Networking by pupils

The school is aware that there are many social media sites that state that they are not for under the age of 13 including Facebook, Instagram, Snapchat and WhatsApp. Facebook is targeted at older teenagers and adults. They have a no under-13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy: "If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that

information as quickly as possible. We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet."

The following are the expectations for all children at St Alban's Primary:

- Pupils must not access social networking sites during the school working day
- Only year 5 and 6 pupils are permitted to bring their mobile phones to school. All mobile phones must be turned off on the school premises and handed into the class teacher at the beginning of the school day. Mobile phones will be stored in the locked drawer of the teachers' desk. Failure to follow this guidance will result in a total ban for the student using a mobile phone.
- Pupils should never attempt to 'friend' or 'follow' staff members on social networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher, and the Behaviour Policy will be followed. Parents will also be informed of any unacceptable use of social media.
- School IT equipment must not be used to access social networking sites at any time of day.
- Any improper use or cyber bullying must be reported to the class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying.
- In order to protect themselves online, St. Alban's pupils must:
    - Never meet anyone in person that they have only communicated with online.
    - Ensure that they don't use their full name – use a nickname or only one of your names. This means only people you really know are likely to find you online.
    - Be aware of other identifiable information in their online profiles –Children must never mention what school they attend, where they carry out hobbies or where they will be at a specific time and place.
    - Ensure that all photos they want to post or send are carefully checked so that they do not include details about them (e.g. football team, school logo, brownies group) and are appropriate.

Code of Conduct: Parents/Carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include School Spider App, the website, School Facebook account, newsletters, letters and verbal discussion. School policies provide further information regarding appropriate channels of communication.
Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for every child. Parents must:
    - Never take phots or videos at school events.
    - Not post pictures of pupils, other than their own children, on social media/networking sites.
    - Make complaints appropriately through official school channels. It is never appropriate to post complaints on social networking sites.
    - Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

Potential and Actual Breaches of the Code of Conduct
In instances where there has been a breach of the above Code of Conduct, the following will apply:
- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken.

- A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from the Governing Body and St. Clare's CMAT where appropriate. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation.

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Pupils

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.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the behaviour policy. No child is permitted to use a mobile phone during school hours and any use of computers is directly supervised by adults. Should a child use any form of technology to bully another child in school, the behaviour policy will be used to guide staff in dealing with the resolutions and consequences.

The school cannot, and will not, be held responsible in any way for the behaviour of pupils online or otherwise, outside of school hours (other than on trips and events agreed and supervised by ourselves). At these times, it is expected that parents/carers closely monitor their child's use of both online media and work with school to safeguard all children using social media, communication apps and online gaming etc out of school.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- Not view the image
- Confiscate the device and report the incident to the headteahcer/DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

Parents

The school shares information 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.

Parents must share instances of cyber-bullying with the DSLs so that it can be addressed. It can also be helpful for parents to inform the school if there is an issue of inappropriate use of online/social media between pupils, so that the school can monitor closely any further behaviour that may need addressing.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy. The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged."

Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:
- Expose (an individual) to hatred, ridicule or contempt
- Cause (an individual) to be shunned or avoided
- Lower (an individual's) standing in the estimation of right thinking members of society or
- Disparage (an individual in their) business, trade, office or profession.
(National Association of Head Teachers)

Staff

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Prevention activities are key to ensuring that staff are also protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance, staff should reduce the risk of personal information falling into the wrong hands.

If cyber-bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Staff are encouraged to report all incidents of cyber-bullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Roles and responsibilities

The Governing Board
The governing board has overall responsibility for monitoring this policy and holding the head teacher 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 ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.

Head Teacher
The head teacher is responsible for ensuring that staff, parents and pupils understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead
Details of the school's designated safeguarding lead (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 all stakeholders understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, computing leader 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 and dealt with appropriately in line with the Online Safety 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.

The Technician
The Technician 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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, 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 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.

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
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    o What are the issues? – UK Safer Internet Centre
    o Hot topics – Childnet International
    o Parent resource sheet – 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.

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. 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.

Pupils using mobile devices in school

Pupils may bring mobile devices into school in year 5 & 6 if they have consent to walk to and from school alone, but they are not permitted to use them during the school day, this includes clubs before or after school, and any other activities organised by the school.

All mobile phones must be handed in to the class teacher at the beginning of the day and pupils will receive them back at the end of the day.

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.

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 by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT technician and inform the school business manager and computing leader.

Monitoring arrangements

All teaching staff log behaviour and safeguarding issues related to online safety on CPOMS. Reviews of these issues are carried out by the DSL frequently.

This policy will be reviewed every year by the computing leader, in partnership with the headteacher. At every review, the policy will be shared with the governing board.

The review will be supported by a 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.

Links with other policies

This online safety policy is linked to our:
- Child protection and safeguarding policy
- Anti-bullying and Behaviour policy
- Computing policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy