St Alban's Catholic High School

Online Safety Policy

2025-2026

Approved by the LGB March 2026

Reviewed March 2027

Introduction

Key people / dates

St Alban's Catholic High School Our Lady of Walsingham Catholic Multi Academy Trust	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Aliyah Harries
	Deputy Designated Safeguarding Leads / DSL Team Members	Jade Block Martin Mirshemirani Adam Millington Helen Arthur Melanie Bush
	Link governor for safeguarding	Austine Adigwe
	Link governor for web filtering	Austine Adigwe
	Curriculum leads with relevance to online safeguarding and their role PSHE & Computing lead	Matthew Summers Ian Robinson
	Network manager / other technical support	SHARP IT
	Date this policy was reviewed	April 2026
	Date of next review	October 2027

Contents

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for the online behaviour, attitudes, activities and use of digital technology (including when devices are offline) by all members of the school community.
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and students for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with students to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of students in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, enhancing learning, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to our other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

This policy applies to all members of the St Alban's Catholic High School community (including teaching, supply and support staff, governors, volunteers, contractors, students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together and may make honest mistakes together and support each other in a world that is online and offline at the same time.

Education and curriculum

Despite the risks associated with being online, St Alban's Catholic High School recognises the opportunities and benefits to students too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, are critical to student's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what students have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help students navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of all students.

The teaching of online safety, features in these particular areas of curriculum delivery:

- Relationships education, relationships and sex education (RSE) and health (also known as PSHE)
- Computing

However, as stated previously, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what students are

doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. For example, saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

We communicate with parents and carers about how we support students with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by regular contact with home, sharing curriculum maps onto our school website, and communicating opportunities for further learning through webinars or reading material.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

The school commits to take all reasonable precautions to safeguard students online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to a Designated Safeguarding Lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on MyConcern. This includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

Any concern/allegation about staff misuse is always (similar to any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for students and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

For more information on reporting channels for online safety concerns, please visit reporting.lgfl.net

The following sub-sections provide detail on managing particular types of concern.

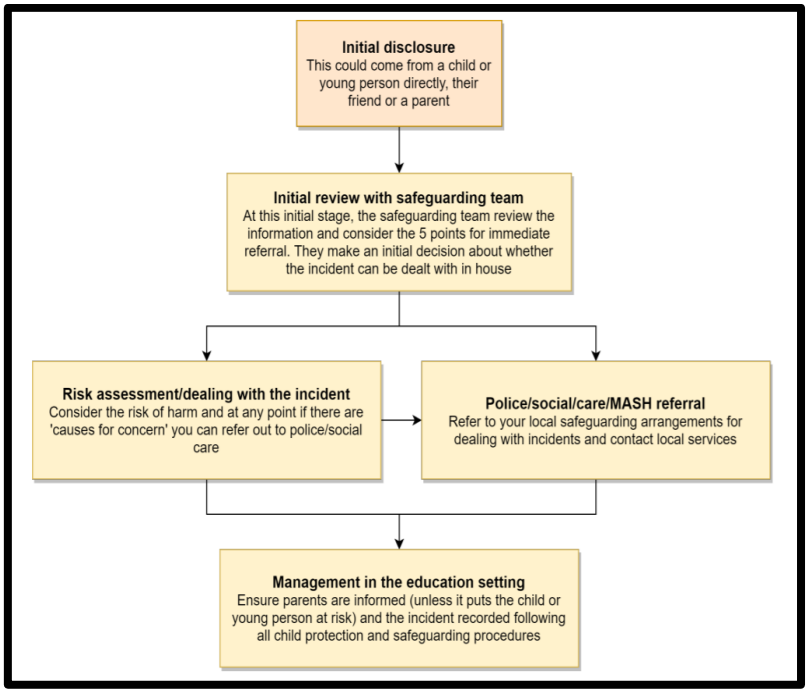
Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

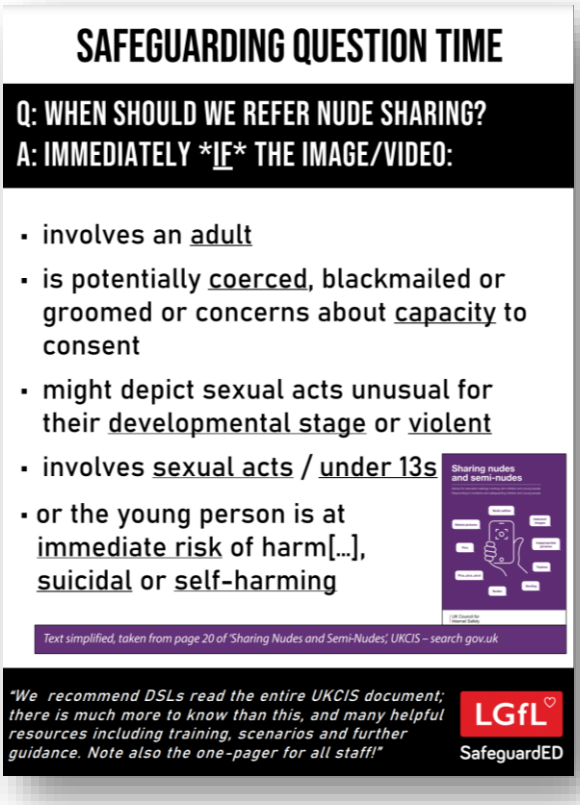
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff must not attempt to view, share or delete the image or ask anyone else to do so, but to go to the DSL immediately**.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting students.



The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:



Priority Areas

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse students/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying and behaviour policy should be followed. This includes issues arising from banter.

The school also recognises that students may communicate via group chats. The school does not encourage this and actively teaches students about the dangers regarding group chats. Where there are issues relating to group chats, the school will take steps to resolve this in line with the behaviour policy.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully students in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. The school will follow its safeguarding and child protection policy for all incidents of child-on-child sexual violence or harassment.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where students contravene these rules, the school behaviour policy will be applied. It will be necessary to reinforce these as usual at the beginning of any school year but also to remind students that **the same applies for any home learning** that may take place.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

The school also works with students to educate and take preventative measures to reduce the misuse of school technology. This can include PSHE sessions, restorative work, the use of Risk Assessments and individual intervention.

Social media incidents

Social media incidents involving students can often cause safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policy and Behaviour Policy.

Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for students and adults in the St Alban's Catholic High School community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), St Alban's Catholic High School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

CCTV

CCTV is used throughout St Alban's Catholic High School. Please see the CCTV policy for more information.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. A copy of the school's PREVENT risk assessment can be found on the school website. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cyber security

All students, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy which can be found on the school website. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard students. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

It is important to remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping students safe. As outlined in *Data protection in schools*, 2023, *"It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child*." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with SHARP IT and Our Lady of Walsingham Catholic Multi Academy Trust to implement the DfE filtering and monitoring standards, which require schools to:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure all staff are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking. They can submit concerns at any point via MyConcern.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum. The Headteacher, DSL, Trust representative and SHARP IT will meet at least annually to review the filtering and monitoring systems in place.

We carry out termly checks to ensure filtering is operational, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

At our school we recognise that generative AI sites can pose data risks, so staff are not allowed to enter student data in these sites and where they use them, they must be approved. For students, we block the

generative AI category and only allow specific sites. We know that what students input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines. Find out more at genaisafe.lgfl.net

Safe Search is enforced on any accessible search engines on all school-managed devices.

Students do not have free access to Youtube. This helps us to limit inappropriate content that is served to students.

Out of hours, our policies are:

- For filtering devices, we have the Lightspeed filtering agent installed on all school devices. This agent continues to strictly filter no matter the location or hours. All devices are built with this agent to ensure they are secure.
- For monitoring devices, Lightspeed and Impero software is installed to each device and is used to monitor devices no matter the location or hours.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via Acceptable Use Policies (AUPs) and regular training reminders in the light of the annual review and regular checks that will be carried out.

The pastoral team checks filtering reports and notifications regularly and takes any necessary action as a result.

According to the DfE standards, "Your monitoring plan should include how you will monitor students when using school-managed devices connected to the internet. This could include:

- Device monitoring using device management software
- In-person monitoring in the classroom
- Network monitoring using log files of internet traffic and web access"

At St Alban's Catholic High School, we use Impero Backdrop to monitor students when using school-managed devices. Impero records all screen content and gives staff the ability to take control, edit and block student access. Impero will also create capture alerts of anything a student might try to access or type that is deemed inappropriate.

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Staff at this school use the email system provided by Microsoft for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with

students or parents, or to colleagues when relating to school/student data, using a non-school-administered system.

- Staff at this school use Arbor and Microsoft Teams to communicate with students and parents/carers.

The systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice, protecting students against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any student login or storing school/student data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a student) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles of messaging/commenting systems

- More detail for all the points below are given in the **Error! Reference source not found.** section of this policy as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy on the school website and only using the authorised systems mentioned above.
- Students and staff are allowed to use the email system for reasonable (not excessive, not during lessons) professional use only but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour always apply. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure). Students are not able to communicate with each other via email.

Use of generative AI

At St Alban's Catholic High School, we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with students, staff and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any student found doing so.
- In school, we allow staff to access Microsoft co-pilot in line with the published Trust guidance note.

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. In St Alban's Catholic High School this includes all Microsoft Office 365 apps.

For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it. Any new platforms will be approved by SHARP IT and the Headteacher.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors may delegate the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

Digital images and video

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

Students of sufficient age and maturity will also be asked to provide their consent to the use of their photos or video in any school related activity.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any students shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored in centralised folders in line with the retention schedule of the school Data Protection Policy. SHARP IT are responsible for checking images/video on all school devices. Any concerns about the nature of these images will be reported to the DSL.

Staff and parents are reminded regularly about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further information on managing student image and video content is available here.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Students are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Our Social Media presence

St Alban's Catholic High School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.

Staff, students' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the Acceptable Use policy which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving students/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, students will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentonlinesafety.lgfl.net and parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the school has official social media accounts, we will not respond to general enquiries about the school or students on these platforms.

The school also recognises that not all information posted online about the school is within its control. The school may periodically review community websites such as Wikipedia to ensure that information is relevant/accurate, with corrections being made to the relevant community owners.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

As outlined in the Acceptable Use Policies, students/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Students/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow any student's public account.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the student or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a student) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on **Error! Reference source not found.**, and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with students or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- The school has a separate Bring Your Own Device Policy which is available via the school website.

- **Students** are permitted to bring phones into school for the purpose of using them to and from school. However, during the school day, phones must remain turned off and in school bags at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the school following its behaviour policy. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to students in emergencies. Our approach to students using mobile phones is in line with DfE, Mobile Phone Guidance.
- Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or students, including remotely, with any device. This also applies to smart watches.
- Staff or students who require a mobile device for the monitoring of medical conditions may do so with the permission of the Headteacher. The school should be informed of any such medical conditions and an Individual Health Plan created.

- **Volunteers, contractors, governors** should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of students or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff. Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or students, including remotely, with any device.
- **Parents** are asked to not use their mobile phones when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the school office. We do not allow Apple AirTags or similar devices in school. Please note that it is against the terms and conditions of these products to use them to track a child.
- Where BYOD is allowed, neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

Use of school devices

Staff and students are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible to staff and sixth form students only for school-related internet use use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with students/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

If on trips students are encouraged to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school and therefore staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher and senior staff authorised by the Headteacher have a statutory power to search students/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.