THE SALTERNS ACADEMY TRUST: ADMIRAL LORD NELSON SCHOOL

Internet Acceptable Use and Social Media Policy

Author:	Martin Fuller
Position:	Assistant Headteacher: Curriculum
Date written:	20th March 2026
Date agreed and ratified by the Governing Body:	29th April 2026
Date of next review:	Annual

CONTENTS **PAGE NUMBER**

Article 17 – UN Convention on the Rights of the Child:
Every child has the right to access reliable information from a variety of sources, and governments must protect children from materials that could harm them.

Scope of this Policy

This policy applies to all members of the school community including students, staff, governors, volunteers, contractors and visitors who access the school's IT systems or use digital technologies within the school environment.

It also applies to the use of school systems off-site and to online behaviour where this may impact the safety, wellbeing or reputation of the school community.

1. Key Staff

Role	**Name(s)**
Headteacher	Chris Doherty
Deputy Headteacher: Quality of Education	Matthew Hutton
Trust IT Network Manager	James Kirk
Online safety Co-Ordinator (Digital Communication Curriculum Director)	Gianni Angio
Deputy Headteacher: Student Achievement/DSL	Katie Holness
Assistant Headteacher: Personal Development	Samantha Easson
Assistant Headteacher: Behaviour and Achievement	Vicky Brown
Assistant Headteacher: Curriculum	Martin Fuller

2. Governors Statement

The Governing Body will ensure that:

- Students and staff will use the internet and digital technologies safely, responsibly and respectfully for educational, personal and recreational purposes.
- Appropriate safeguards will be in place to protect the school's network, devices and users from accidental misuse, deliberate misuse, cyber threats and other security risks.
- The school will provide appropriate access to digital technologies to support learning and teaching. In return, students and staff are expected to act as responsible users and follow the school's Internet Acceptable Use and Social Media Policy.

3. Rationale

Digital technologies are an integral part of modern life both within and beyond school. They provide powerful opportunities to support teaching, learning, creativity and communication. When used effectively, digital technologies can enhance engagement, stimulate discussion and support students in developing knowledge, skills and understanding in a wide range of contexts. Students are therefore entitled to access the internet in a way that is safe, appropriate and supportive of learning.

Online safety is recognised as a key safeguarding responsibility and forms part of the school's wider approach to protecting students from harm both within and beyond the school environment. The use of technology is also a significant feature of many contemporary safeguarding issues. Risks such as child sexual exploitation, online grooming, sexual predation, cyberbullying and radicalisation may be facilitated through digital platforms. An effective approach to online safety therefore enables the school to both protect and educate the whole school community, ensuring that students and staff understand how to use technology safely and responsibly. It also ensures that there are clear systems in place to identify, report, respond to and escalate concerns where appropriate.

For the purpose of this policy, social media refers to digital platforms, applications and websites that enable users to create, share and interact with content online. This includes services accessed through computers, tablets and mobile devices, such as messaging services, social networking sites, online forums, blogs and video-sharing platforms. Examples may include platforms such as Facebook, Instagram, TikTok, Snapchat, X (formerly Twitter) and YouTube, although new services continue to emerge.

The widespread availability of social media provides valuable opportunities for communication, collaboration and learning. However, its use must be balanced with the responsibility to maintain appropriate online conduct, protect personal information, comply with legal and safeguarding responsibilities, and safeguard the reputation of the school and its community.

The school recognises that some students, including those who are disadvantaged, have special educational needs and disabilities (SEND), or are children we care for, may require additional support in developing safe and responsible online behaviours. When digital technologies are used inappropriately, these students may be particularly vulnerable to harm. The school will therefore ensure that appropriate guidance, education and support are provided so that all students can use digital technologies safely and confidently.

4. Aims

This Policy is intended to ensure:

- young people and staff will be responsible users and stay safe while using the internet and social media platforms for educational, personal and recreational use.
- school systems and users are protected from accidental, deliberate misuse, cyber threats and other security risks that could put the security of the systems and users at risk.

Admiral Lord Nelson School will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect students to agree to be responsible users.

It is not possible to eliminate all risks, so it is important that users' understanding of the risks to which they may be exposed is built through good education and training provision so that they have the confidence and skills to face and deal with them.

Under the Education and Inspections Act 2006, the Headteacher has the authority to regulate the behaviour of students even when they are not at school. This includes the power to apply disciplinary consequences where off-site behaviour, including cyberbullying or other online behaviour, has an impact on the safety, wellbeing or reputation of the school community.

5. Roles and Responsibilities

Deputy Headteacher: Quality of Education
The Deputy Headteacher: Curriculum Design will;

- Lead the annual review of the Internet Acceptable Use and Social Media Policy consulting with the Assistant Headteacher; Student Achievement**,** the Designated Safeguarding lead (DSL), the Online safety coordinator, the Trust Network Manager and the Senior Leader; Personal Development;
- Ensure the policy is shared and then ratified by the School Governors;
- Ensure the policy is shared with all ALNS staff and implemented across the school.

Designated Safeguarding Lead (DSL)/ Deputy Headteacher: Student Achievement
The Designated Safeguarding Lead (DSL) will;

- Maintain an up-to-date understanding of developments in online safety;
- Co-ordinate a response any alleged online safety incident and establish evidence of any breach or wrongdoing in conjunction with the Assistant Headteacher; Student Achievement and Behaviour;
- Ensure that all new staff receive online safety training as part of their induction programme,
- Ensure existing staff fully understand Internet Acceptable Use and Social Media Policy.
- Ensure a holistic response to changing patterns and/or behaviours causing concern, including consideration of vulnerable student groups such as those with SEND or who are Children Looked After(CLA).
- Co-construct the school online safety education programme for students, staff, parents and governors;

- Maintain a record of online safety incidents reported as safeguarding concerns and the actions taken via CPOMS;
- Liaise with the Senior Leader Personal Development and Heads of House where necessary Assistant Headteacher; Student Achievement and Behaviour
- Routinely monitor student online behaviours through technologies such as web filtering and monitoring systems including SENSO.

Assistant Headteacher: Student Achievement and Behaviour
The Assistant Headteacher: Student Achievement and Behaviour will;

- Maintain an up-to-date understanding of developments in online safety;
- Ensure a holistic response to changing patterns and/or behaviours causing concern.
- Co-ordinate a response to any alleged online safety incident and establish evidence of any breach or wrongdoing and co-ordinate any response in conjunction with the DSL;
- Liaise with the DSL, AHT Personal Development and the Heads of House where necessary;

Assistant Headteacher: Curriculum (Online Safety Policy Lead)
The Assistant Headteacher: Curriculum will;

- Lead the drafting, implementation and ongoing development of the Internet Acceptable Use and Social Media Policy, ensuring it reflects current statutory guidance including KCSIE and DfE Filtering and Monitoring Standards;
- Ensure the policy is consistently implemented across the school, with particular focus on classroom practice, staff expectations and student use of technology;
- Work in collaboration with the DSL, Trust Network Manager and Online Safety Co-ordinator to ensure a joined-up and proactive approach to online safety;
- Ensure staff understand and apply expectations consistently, including through CPD, briefing and clear systems;
- Report to Governors and SLT on the effectiveness of online safety provision, including strengths, areas for development and emerging risks.

Assistant Headteacher: Personal Development
The school has a designated AHT as the Personal Development Co-ordinator and they will;

- Map the delivery of online safety across the AF and Personal Development Curriculum.
- Co-ordinate the school online safety education programme in conjunction with online safety coordinator and Aspiring Futures (PSHEE) Co-ordinator.
- Maintain an up-to-date understanding of developments in online safety, seeking student voice to inform decisions around content for Personal Development delivery

Online Safety Co-Ordinator (Digital Communication Curriculum Director)
The school has a senior member with the responsibility as the Digital Communication Curriculum Director. They fulfil the following roles as the online safety Co-ordinator and will;

- Maintain an up-to-date understanding of developments in online safety; ensuring that student voice is sought in this and as a result the curriculum is kept up to date
- Liaise with Trust Network Manager and the DSL over online safety concerns to ensure a holistic response;

- Co-construct the school online safety education programme for students, staff, parents and governors;
- Liaise with the DSL and Heads of House where necessary;

Trust Network Manager

The Trust Network Manager will;

- Maintain an up-to-date understanding of developments in online safety;
- Audit the online safety training needs of all staff to be carried out annually;
- Liaise with the Online safety coordinator, the Senior Leader Personal Development and Heads of House where necessary;
- Ensure Filtering and Monitoring Standards (as specified by the DFE in March 2023) are met and reviewed annually.

School staff

All school staff will;

- Make themselves aware of this policy's content and successfully complete any relevant E- safety training required by the school.
- Be responsible for contributing to the positive re-enforcement of safe behaviours through their day-to-day interaction with students and technology, reinforcing the 4 Cs message often (Content, Commerce, Conduct and Contact)
- Be proactive in monitoring student on-line behavior in lessons using SENSO (Cloud- Based Platform for. Device Monitoring and Management) to ensure that internet access is for legitimate educational purposes and not for texting, accessing social networking sites or recording audio, video or still imagery without permission.
- Ensure that appropriate online safety information and materials are readily available for students use. For example, through posters, the school's website, social media and/or learning platforms.
- Act as good role models in their use of IT, the Internet and mobile devices.
- Monitor the online safety tools and report any vulnerabilities to their line manager and the IT support team and/or Trust Network Manager.

Students

All school students will;

- Use school IT systems for educational purpose
- Respect others online and not engage in cyberbullying
- Keep passwords secure
- Report inappropriate content or contact
- Follow school rules regarding devices and internet access
- Not deliberately damage, misuse, or attempt to interfere with any school hardware, software, devices, networks, or digital infrastructure, including Chromebooks and other school-owned equipment. Failure to follow these expectations may result in disciplinary action in line with the school's behaviour policy.

6. Monitoring

Admiral Lord Nelson School will annually review and monitor the impact of the policy using:

- Logs of reported incidents reported in termly Behaviour reports to Governors on MIS.
- Internal monitoring of user data, such as web filtering logs, search engine queries and web-browsing history;
- Surveys/ questionnaires of users;
- The Trust Network Manager and online safety coordinator attend appropriate training and networking events to ensure the organisation is able to respond to emerging safety concerns and technical changes.
- External cyber security audits of school IT internet and network with the risks and actions quality assured by the Saltern Trust Board Risk Committee.

7. Online Safety Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the online safety provision at ALNS. Students need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be referenced in all areas of the curriculum and staff should reinforce online safety messages whenever IT is being used (via – Content, Conduct, Contact, Commerce)

A planned online safety programme will be provided as part of both IT and Aspiring Futures (PSHEE) lessons and will be regularly revisited – this will cover the use of IT both in and outside school and will include.

- The safe and responsible use of the Internet
- The safe and responsible use of mobile devices
- The safe and responsible use of social media
- The management of digital identity

Key online safety messages will be reinforced as part of a planned programme of assemblies and tutor activities.

In lessons where the Internet is accessed, it is best practice that students be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

It is accepted that students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request a temporary removal of those sites from the filtered list, for the period of study by email to ITHelpdesk@alns.co.uk and should be auditable, time-limited and with clear reasons given.

Whenever the Internet is used for research, students should be taught to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Equally, students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet. This is a critical cross-curricular responsibility.

Students should be helped to understand the need for an Internet Acceptable Use and Social Media Policy and be encouraged to adopt safe and responsible use of IT, the Internet and mobile devices both within and outside the school.

Parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of their children's on-line experiences. Parents can often either underestimate or do not realise how often young people come across potentially harmful and inappropriate material on the Internet and can be unsure about what they should do about it.

Admiral Lord Nelson School will therefore seek to provide information and awareness to parents and carers through:

- Letters, weekly bulletins, social media platforms and school website;
- Annual Parent Information Evenings.
- Termly Safeguarding bulletin

As part of the long-term teaching and learning strategy most students (80%+) at school have a leased Chromebook provided by FreedomTech.

Schools also recognise that artificial intelligence (AI) and generative AI tools are becoming increasingly available to students. Where such tools are used, students must use them responsibly and in line with school expectations regarding academic integrity, data protection and safe use of technology. This is covered in full in our AI policy.

- At Salterns academy Trust], we embrace Artificial Intelligence (AI) as a tool to enhance
- learning, support teaching, and streamline administrative tasks. Our approach is guided by
- the Trusts AI Policy, ensuring that AI is used responsibly, safely, and ethically.
- Why we use AI:
- To help teachers save time on administrative tasks, so they can focus on teaching.
- To develop students' digital literacy, critical thinking, and understanding of AI.
- To improve accessibility and inclusion for all learners.
- How we use AI safely:
- Staff are aware of their responsibilities with regard to AI use, guided by our AI
- Acceptable Use Agreements.
- Sensitive information about pupils, staff, or families is only entered into AI tools with
- explicit authorisation and robust security measures. Copilot with Enterprise data
- protection is our approved AI tool for this purpose
- AI outputs are always checked by humans. AI assists, it does not replace professional
- judgment.
- We are transparent about when AI has been used in communications, teaching
- materials, or administrative tasks.
- Working with Parents and Carers:
- AI may be used to support communication, such as drafting newsletters or summarising
- pupil progress.
- All AI-assisted communication is reviewed to ensure it is accurate, professional, and
- respects privacy.
- Parents and carers are encouraged to discuss any concerns or questions about AI use
- with the school.
- Supporting learners:
- Students are guided to use AI safely, ethically, and creatively.
- AI is a learning aid, not a replacement for students' own thinking or work.
- Resources and guidance are provided to ensure all students benefit equitably from AI.

8. Online Safety Staff Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

The DSL should ensure that all new staff receive online safety training as part of their induction programme, It is important that both new and existing staff fully understand Internet Acceptable Use and Social Media Policy. It is also referenced in the Staff Code of Conduct Policy which all staff sign to say they have read and agree to on an annual basis or on induction.

An audit of the online safety training needs of all staff will be carried out annually administered by the Trust IT Manager.

The DSL and IT Services team (under the guidance of the Trust Network Manager) will provide advice/guidance/training to individuals as required.

School staff are provided with online training modules throughout the school year. Cyber Awareness Training & Phishing Simulations | Boxphish

Staff training will also ensure that all staff understand their safeguarding responsibilities in relation to online safety and are able to recognise, respond to and report concerns in line with the school's safeguarding procedures.

The assigned Governor with the responsibility for safeguarding should take part in online safety training/ awareness sessions. This may be offered in variety of ways:

- Attendance and/or completion of any online safety staff training;
- Participation in information sessions for staff or parents

9. Responding to Online Safety Incidents

Admiral Lord Nelson School will ensure that there are effective safeguarding systems in place for students and staff to report any concerns that may arise. If the incident is of a safeguarding nature this incident should be reported directly to the DSL and logged on CPOMS. If the matter is not considered a safeguarding issue, it should be reported to the Head of House and Line Manager on Class Charts.

The DSL or HoH will;

- Liaise with the member of staff reporting the incident and establish evidence of any breach or wrongdoing
- Direct any work with any students involved to resolve issues and educate users as necessary, inform parents / carers of the incident and any outcomes
- Where the alleged incident involves staff misuse, the Headteacher must be informed.

Outcomes of investigations will be reported to the Headteacher and to external services where appropriate (e.g. Social Services, Police, the Child Exploitation and Online Protection Service).

10. Cyber Security

Salterns Trust will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented:

- There will be regular reviews and audits of the safety and security of IT systems, using external resources where required;
- Appropriate security measures are in place to protect infrastructure and end-user devices from unauthorised access, accidental damage or malicious intent which might threaten the safety of users and/or the security of systems and data.
- Monthly systematic network/infrastructure checks take place by the IT services team and are logged;
- All users will have clearly defined access rights to the IT systems in line with GDPR principles. This will be defined and accountable by the Trust Network Manager in conjunction Student Services Team Manager;
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to *IThelpdesk.alns.@salterns.org* ;
- Admiral Lord Nelson School will use a sufficient Internet filtering system to restrict IT access to certain materials, adhering to current government guidelines and recommendations;
- Filtering and monitoring systems will be reviewed annualy to ensure they remain effective in safeguarding students and supporting safe use of technology.
- Admiral Lord Nelson School will reserve the right to use internal monitoring systems to intercept and record any IT use for safeguarding and security purposes;
- Remote management tools may be used by staff to control workstations and view users' activity;
- Admiral Lord Nelson School will use 3rd party companies where necessary, to provide user testing and training, such as monthly Phishing email campaigns.

11. Responding to Cyber Security Incidents/Concerns

Salterns Trust will ensure that there are effective cyber security measures in place as identified and recommended from external cyber security audits and reviews.

Staff must immediately report any suspicion or evidence that there has been a breach of security to IThelpdesk.alns.@salterns.org. If the incident is of a serious nature this incident should be reported directly to the Headteacher or in their absence a Deputy Headteacher. All cyber security incidents must also be reported to the Trust, who will work with external cyber security advisers or relevant authorities as necessary.

The Trust Network Manager will;

- *Liaise with the member of staff reporting the incident and then, if deemed serious, inform the Headteacher to consider any necessary immediate action.*

- *Where the alleged threat involves staff misuse, the Headteacher must be informed,*
- *Outcomes of investigation and actions will be reported* to the Headteacher.

12. Staff Personal Use of Social Media

Working in a school, requires all staff to maintain professional boundaries in all forms of communication whether it involves electronic/digital technology or not. This is vital to maintain public trust and appropriate professional relationships with students. Our conduct inside or outside of work should not lead us to blur or cross those professional boundaries.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006, the Malicious Communications Act 1988 and other legislation. They must also operate in line with the school's Equalities at ALNS and Child Protection and Safeguarding policies.

The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites during designated breaks only.

The principles below are to help staff to mitigate the potential risks of using social media. The principles apply to any approved use of social media communication within the school or to personal use of social media outside of school.

It applies to all staff, including casual/supply staff, volunteers, governors, or anyone working within the school and using the school's systems and equipment whether on or off the premises. This document should be read with the School Staff Code of Conduct and Child Protection and Safeguarding Policy.

Basic principles in managing staff personal use of Social Media:

- "Nothing" on social media is truly private;
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts;
- Keep an eye on your digital footprint;
- Keep your personal information private;
- Regularly review your connections – keep them to those you want to be connected to;
- When posting online consider; Scale, Audience and Permanency of what you post;
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem;
- Consider refraining from identifying themselves as working for the school as posted content could bring the school into disrepute;
- Take care that their interaction on social media does not damage working relationships between members of staff, students at the school, their families and other stakeholders and/or working partners of the school;
- Maintain professional standards by communicating with student & parents/carers electronically at appropriate times of the day and through established approved channels e.g. school approved email or approved social media platforms (for example, ALNS Facebook Page or ALNS Parents Facebook page);
- Do not exchange private texts, phone numbers, personal email addresses or photos of a personal nature with students/parents or carers;
- Staff must not communicate with students through personal messaging platforms or social media applications (for example WhatsApp, Snapchat, Instagram, Discord or similar). Communication with students must only take place through school-approved systems and platforms;
- Staff should ensure that any use of artificial intelligence or digital assistance tools when communicating professionally does not involve sharing personal, safeguarding or confidential school information;
- Maintain a formal, courteous and professional tone in all communications to ensure that professional boundaries are maintained;
- Manage the privacy and security settings of your social media accounts. Privacy settings can shift and change without notice. Check the settings frequently.
- Ensure that privacy settings for content/photos are set appropriately and monitor who can post to your social media locations and view what you post.

- Protect yourself from identity theft by restricting the amount of personal information that you give out. Be cautious about posting detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords and enable personal details to be cloned for fraudulent acts etc and grooming.
- Do not post comments which incite others to make discriminatory or other professionally unacceptable comments;
- Do not post school logos or similar images that may lead readers of posts etc. to believe the staff member is speaking on behalf of the school.
- Do not accept any current student of any age or as a friend, follower, subscriber or similar on any personal social media account. In some exceptional circumstances interaction on social media may be appropriate e.g. members of the same family. Additionally, staff must never contact ex-students using social media platforms until they reach the age of 18 and then it is strongly advised against and staff must inform their line manager as to the purpose of the social media contact.
- Do not bully or harass any colleagues via social media sites. Any allegations will be dealt with under the schools' normal disciplinary procedures.
- Do not incite racial or religious hatred or similar activities – these may lead to criminal investigations and penalties;
- Do not post libelous statements – an individual may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by a staff member could mean the school is vicariously liable for defamatory statements if carried out in the normal course of employment, even if performed without the consent or approval of the school. Similarly, making such statements on your own initiative and not at work could lead to legal action

13. Staff Use of Approved School Social Media Platforms

ALNS staff must <u>not</u>:

- Disclose confidential and personal information without express authority especially about students, parents or carers, staff, voluntary or other workers at the school nor breach their right to privacy;
- Engage in posts or activities which are detrimental to maintaining effective working relationships between individuals 'working' at the school;
- Bring the reputation of the school into disrepute;
- Engage in activities which compromise, or might be seen to compromise, the professional standards of teaching or the professional standards applicable to support staff;
- Share information with students or parents/carers in any environment they would not willingly and appropriately share in a school or school-related setting or in the community.
- Please read see APPENDIX 2 – APPROVED SOCIAL MEDIA PLATFORM PROTOCOLS

There are many legitimate uses of social media within the curriculum and to support student learning.
There are many possibilities for using social media to enhance and develop students' learning. However, when using social media, the boundaries between professional and personal can become more blurred and users can unwittingly or wittingly publish things they may later regret. Published items can be capable of more than one interpretation but once published the damage may not be recoverable. Staff using approved school social media platforms must ensure that communication remains professional and appropriate at all times.

14. Respecting Confidentiality and Copyright

The disclosure of confidential information about the school or individuals associated with the school may breach their right to privacy.

- Don't publish anything that might allow inferences to be drawn which could embarrass or damage a student, employee, governor, volunteer or supplier.
- Breaches of copyright or other similar infringements – passing on text, photos etc; may infringe the owner's copyright. Always ensure that you have the permission of the owner.

The school takes the matters above seriously and disciplinary action will be taken. A very serious view will also be taken of any individual who ignores or wilfully or carelessly carries out actions or omits to act which results in breaches of the instructions and advice contained in this policy and the result is for example, undermining effective working relationships, professional boundaries between staff and student etc.

15. Feeling Aggrieved or Concerned About Matters at Work

If staff feel that an unfair decision has been made or that malpractice is occurring staff should not post personal feelings on-line, which are likely to be impulsive, inappropriate, or heated comments. This may lead to the staff member being part of the problem. Instead, staff must speak directly to their line manager or if that is not appropriate, directly to HR@salterns.org. If neither of these are appropriate staff can refer the matter to the Deputy Headteachers and/or the Headteacher. If this too is not appropriate, staff should refer to the ALNS Grievance Policy.

16. Reporting Inappropriate or Concerning Online Behaviour

If a staff member becomes aware of inappropriate material/comments they should notify the DSL as soon as possible and provide screenshots of the comments made, if possible.

If a student makes 'social' or inappropriate contact with a staff member, the staff member must notify the DSL as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a student, the incident must be notified to the Designated Safeguarding Lead as soon as possible. The school can then deal with the situation as appropriate. Where appropriate, incidents may also be referred to external agencies including the Local Authority, Police or relevant online safety reporting services.

17. Breaches of Policy

Any violation of the standards, procedures or guidelines set out in this policy may be treated as a formal disciplinary matter, which could result in dismissal, legal prosecution or both.

18. Other Relevant Policies and Guidance

- Anti-bullying Policy
- Child Protection and Safeguarding Policy
- Trust Data Protection Policy
- Trust Grievance Policy
- Relationships and Behaviour Systems Policy
- Trust Privacy Notice for Students
- Trust Privacy Notice for Parents and Carers
- Trust Privacy Notice for Parents and Carers – use of your child's personal data
  (All the above policies can be found here: https://alns.co.uk/school-policies/)
- ALNS Staff Code of Conduct

19. Useful Links

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
- Keeping children safe in education - GOV.UK
- Searching, Screening and Confiscation
- https://www.gov.uk/government/publications/teaching-onlinonline safety-in-schools
- Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

APPENDIX 1 - ACCEPTABLE USE AGREEMENT FOR DIGITAL TECHNOLOGIES USER

GUIDANCE
All ALNS users are required to read and then confirm they read this agreement at the start of each academic year or during the year should users arrive mid-academic year.

VISION
We believe that digital technologies can be used to help you to enhance your learning. We want you to be able to employ digital technologies safely, effectively and ethically.

DIGITAL TECHNOLOGIES
This agreement includes all devices and data connected to the school network or brought onto the school site. Examples of what we mean by this include:

- school devices, whether you use them on or off-site. For example: desktop PCs, laptops, leased Chromebooks, tablets, video cameras;
- data on the school's network. For example, your school Google drive, your Office 365 account and your Class Charts account;
- your school email account;
- the use of Remote Desktop which you use to access the school's systems from off-site;
- the school's Wi-Fi.

USE OF DIGITAL TECHNOLOGIES
The agreement sets out the expectations of students regarding digital technologies. By accepting this agreement, you agree to the following statements:

- I will use digital technologies appropriately and only for educational purposes.
- I will only access the school systems with my own username and password.
- I will create a secure password what I will not share this with anyone else.
- I will communicate with others respectfully. This means I will use appropriate language and ensure that my digital activity does not hurt, upset or offend anyone else.
- I will report any concerns, misuse or inappropriate material I come across to a teacher.
- I will report any damage to equipment to a member of staff as soon as it's noticed.
- I will ask the permission of a teacher before making or using any recordings of other students, visitors or staff (whether photographic, audio or video).
- I will not upload any school resources, information, recordings, or the work of others outside the school network without seeking permission from a member of staff (for example YouTube, Instagram, Facebook, Tik Tok etc.)
- As a member of this school community, I will ensure that my online activity, both on and off-site, doesn't bring the school into disrepute.
- I will not seek to bypass any of the school network's security systems (e.g. using VPNs, proxy servers, or attempting to hack other users' passwords).
- I will not download, store, or install software or games onto the school network.
- I will respect the copyright of proprietary material.
- I understand that the school monitors the use of digital technologies by all users.
- I understand that if I break this agreement, consequences may be applied and my parents and carers contacted.

If you are unsure about any of these statements, please ask speak to your line manager for clarification.

APPENDIX 2 – APPROVED SOCIAL MEDIA PLATFORM PROTOCOLS

The school community is encouraged to consider if a social media account will help them in their work, e.g. a History department Twitter account, or a "Friends of the School" Facebook page. Anyone wishing to create such an account must present a business case to the Senior Leadership Team which covers the following points:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will manage the account (at least two staff members should be named)
- Plans for the account to be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and guidance and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently by the assigned manager(s) (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

If the account is not active for a period of time, e.g. summer holidays, it is recommended that the account is frozen to prevent any issues that may arise with an account that is not monitored.

Behaviour

The school requires that all users using social media adhere to the standard of behaviour as set out in the Internet Acceptable use and Social Media Policy and other relevant policies.

Social Media communications by staff must always be professional and respectful and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure confidentiality is maintained on social media even after they leave the school.

Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

If a journalist contacts posts made using social media, refer to a Deputy Headteacher or the Headteacher before responding.

Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

Legal considerations

Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.

If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

If you or someone else is subject to abuse by colleagues through a social networking site, this action must be reported using the agreed school protocols.

Tone of communication

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are, Engaging, Conversational, Informative, Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to – see Appendix 3

Permission to use any photos or video recordings should be sought. If anyone asks not to be filmed or photographed, their wishes should be respected. The names of those
students whose parents have not given permission for their child's image to be included in any photos/films can be found in the public drive of the school network - Image permissions. The list is maintained by the Students Service team.

Under no circumstances should staff share or upload student/student images online other than via school owned social media accounts

Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

If a member of staff inadvertently takes a compromising image which could be misconstrued or misused, they must delete it immediately.

Monitoring posts

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

The school should effectively respond to social media comments outlined below; Staff must:

- check with a senior leader before publishing content that may have controversial implications for the school
- use a disclaimer when expressing personal views
- make it clear who is posting content
- use an appropriate and professional tone
- be respectful to all parties
- ensure you have permission to 'share' other peoples' materials and acknowledge the author
- express opinions but do so in a balanced and measured manner
- think before responding to comments and, when in doubt, get a second opinion
- seek advice and report any mistakes using the school's reporting process
- turn off tagging people in images where possible

Staff must not:

- make comments, post content or link to materials that will bring the school into disrepute
- publish confidential or commercially sensitive material
- breach copyright, data protection or other relevant legislation
- link to, embed or add, potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- post derogatory, defamatory, offensive, harassing or discriminatory content
- use social media to air internal grievances
- Ensure that no information is made available that could provide a person with unauthorised access to the school, its systems and/or any confidential information.
- Not post. any confidential information regarding the school on any social networking website.

APPENDIX 3 – PROTOCOL FOR USE OF STUDENT IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term, e.g. there are many reported incidents of employers carrying out Internet searches for information about potential and existing employees.

ALNS staff must follow these guidelines when considering using student images;

- When creating digital images in lessons, all staff re-enforce students' understanding of the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the Internet;
- Allow staff to take digital/video images to support internal educational use only. Such images should only be recorded using school equipment; personal digital equipment belonging to staff should NOT be used for such purposes;
- Ensure care is taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Digital/video images published on the school website or elsewhere that include students will be selected carefully by staff, and the appropriate checks and permissions will be sought prior to publishing;
- Students' full names will not be used anywhere on the public website. This is to prevent third parties from identifying that a particular individual attends the school. Forenames and year can be used, e.g. "Ben, Year 10";
- Appropriate permission from parents or carers will be obtained before images of students are published on the school website. A list of those students whose image should not be used can be found in the public drive of the school network - Image permissions. The list is maintained by the Students Service team;
- Images should not be passed to a third party for any purpose outside of previously arranged data-processing purposes.
- AI tools must not be used to create, alter, or manipulate images of students, staff, or others without explicit permission**.**