VOYAGE LEARNING CAMPUS

Voyage Learning Campus

ICT AND INTERNET ACCEPTABLE USE POLICY

This policy has been adopted by the Senior Leadership Team on:	
Date adopted:	10th December 2025
Signed:	
Next review due:	December 2027

Contents

---

1. Introduction and aims

Information and communication technology (ICT) is an integral part of the way Voyage Learning Campus operates. It is a critical resource for students, staff, the Management Committee, volunteers and visitors, supporting teaching, learning, safeguarding, and administration across all phases.

While ICT provides significant educational and operational benefits, it also presents potential risks to data security, online safety and safeguarding. This policy sets out how the school manages those risks and ensures that all ICT use is responsible, lawful and aligned with national expectations.

This policy aims to:

- **Set out clear expectations for the safe and responsible use of the school's ICT systems and equipment**
- **Establish consistent standards for online communication and collaboration across the school community**
- **Support and complement the school's policies on Data Protection, Online Safety, and Safeguarding**
- **Prevent disruption, misuse or security breaches within the school's ICT environment**
- **Promote effective digital literacy and safe technology use for all students and staff**

This policy aligns with the **Department for Education's Meeting digital and technology standards in schools and colleges (2024)** and the **National Cyber Security Centre (NCSC) Cyber Security Standards for Schools (2024)**.

Breaches of this policy may be dealt with under the school's Relationships and Behaviour Policy (for students) and Staff Code of Conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- **Data Protection Act 2018**
- **The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020**
- **Computer Misuse Act 1990**
- **Human Rights Act 1998**
- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
- **Education Act 2011**

- **Freedom of Information Act 2000**
- **The Education and Inspections Act 2006**
- **Keeping Children Safe in Education 2025**
- **Searching, screening and confiscation: advice for schools**
- **National Cyber Security Centre (NCSC): Cyber Security for Schools**
- **Education and Training (Welfare of Children) Act 2021**
- **UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people**
- **DfE Filtering and Monitoring Standards for schools and colleges (2023)**
- **DfE Meeting digital and technology standards in schools and colleges (2024)**
- **National Cyber Security Centre (NCSC): Cyber Security Standards for Schools (2024)**
- **DfE Using AI in education settings: support materials" (2025)**

3. Definitions

- ICT facilities: All school-owned or managed digital systems, devices and services, including network infrastructure, computers, laptops, tablets, mobile phones, interactive screens, software, cloud-based systems, websites, web applications and any future technologies provided as part of the school's ICT service.
- Users: Anyone authorised by the school to access or use the ICT facilities, including the Management Committee, staff, students, agency and temporary workers, volunteers, contractors and visitors.
- Personal use: Any use or activity not directly related to a user's role, study or approved school purpose.
- Authorised personnel: Employees or contractors authorised by the school to administer, maintain or monitor the ICT facilities.
- Materials: Any digital content or data created or stored using the school's ICT facilities, including but not limited to documents, photos, audio, video, printed output, web pages, and social-media content.
- Filtering and Monitoring: Technical and procedural controls that restrict access to harmful or inappropriate online material and monitor user activity to identify potential safeguarding or security concerns, in line with the DfE Filtering and Monitoring Standards (2023).
- Artificial Intelligence (AI): Computer systems capable of generating or analysing content such as text, images, video or audio in a human-like way (for example, ChatGPT or Google Gemini). AI use within school must be risk-assessed and comply with data-protection and safeguarding requirements.
- CPOMS: The school's electronic safeguarding and behaviour-management system used to record and track safeguarding, behaviour and online-safety concerns.

4. Unacceptable use

The following activities are considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in action under the Relationships and Behaviour Policy, Staff Code of Conduct, or Disciplinary Policy.

Unacceptable use includes, but is not limited to:

- Using the school's ICT facilities to breach copyright or intellectual-property rights.
- Using the school's ICT facilities to bully, harass, or discriminate against others, including through social-media or messaging platforms.
- Accessing, creating, storing, linking to, or sending material that is illegal, pornographic, obscene, violent, hateful, extremist, or otherwise inappropriate.
- Sharing, requesting, or possessing nude or semi-nude images or videos (consensual or non-consensual).
- Engaging in or promoting unlawful activity, including radicalisation, extremism, or discrimination of any kind.
- Using offensive, threatening, or discriminatory language online.

- Participating in online gambling, scams, or fraudulent or misleading advertising.
- Using generative artificial intelligence (AI) tools (for example, ChatGPT, Copilot, or Google Gemini) to create, share, or distribute harmful, discriminatory, defamatory, or misleading material, including deepfakes or misinformation.
- Downloading, installing, or executing unauthorised software, applications, or scripts, including those that could introduce malware, spyware, or ransomware.
- Attempting to disable, circumvent, or interfere with the school's filtering or monitoring systems.
- Connecting any personal or unauthorised device to the network without approval, or using personal hotspots or tethering to avoid the school network.
- Gaining or attempting to gain unauthorised access to accounts, systems, or restricted information.
- Allowing or encouraging others to gain unauthorised access to the school's ICT systems.
- Accessing, modifying, or sharing data (including personal data) without authorisation, or causing a data breach through negligence or deliberate action.
- Sharing confidential information about the school, its students, staff, or wider community without authorisation.
- Posting, sharing, or forwarding content that could damage the reputation of Voyage Learning Campus.
- Promoting a personal or external business interest unless authorised by the Principal.
- Intentionally damaging, deleting, or disposing of ICT equipment, systems, programs, or data without permission.
- Using any websites, VPNs, or other mechanisms to bypass the school's security or filtering controls.
- Breaching other school policies or procedures relating to behaviour, safeguarding, or data protection.

This list is not exhaustive. The Principal, Vice Principal, Senior Leadership Team, or Online Learning Manager will determine, using professional judgement, whether other behavior's constitute unacceptable use of the school's ICT facilities.

These expectations apply both in and outside of school, including when using personal devices or accounts that could impact other members of the school community.

4.1 Exceptions from unacceptable use

In limited circumstances, the use of the school's ICT facilities may be required for a purpose that would otherwise be considered unacceptable (for example, to support curriculum delivery or technical testing).

Any such exception must be requested in writing and approved in advance by the Principal. The request must explain the purpose, duration, and controls in place to minimise risk.

Approved exceptions will be time-limited, risk-assessed, and logged by the Online Learning Manager for audit and review in line with the DfE Filtering and Monitoring Standards (2023).

4.2 Consequences

Students, staff, and other users who engage in any unacceptable activity listed in this policy may face disciplinary action in line with the school's relevant policies, including:

- Relationships and Behaviour Policy
- Staff Code of Conduct
- Disciplinary Policy

All online-safety incidents and breaches will be recorded on CPOMS and reviewed by the Designated Safeguarding Lead (DSL) and Online Learning Manager to determine appropriate follow-up.

Serious or deliberate breaches, such as accessing illegal content, data compromise, or cyber-security incidents, may result in suspension of access privileges and referral to external agencies, including the police, Local Authority Designated Officer (LADO), or Department for Education, as appropriate.

5. Staff (including Management Committee, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's Online Learning Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the School Business Manager, Principal or Online Learning Manager by email.

All staff must use multi-factor authentication (MFA) for school accounts where available, encrypt sensitive data, and store files securely. Use of password managers for secure credential storage is encouraged.

These responsibilities reflect the expectations set out in the DfE Meeting digital and technology standards in schools and colleges (2024) and the NCSC Cyber Security Standards for Schools (2024).

5.1.1 Use of phones and email

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parent/carers and students, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Staff should remain alert to phishing or social-engineering emails and report any suspicious messages to the Online Learning Manager.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error which contains the personal information of another person, they must inform the Online Learning Manager immediately and follow the data breach procedure found in our Data Protection policy.
- Staff must not give their personal phone numbers to parent/carers or students. Staff who use personal mobile phones to call parent/carers must ensure that show caller ID is turned off and must not use SMS or other messaging services as this could expose their personal phone number.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.
- The school can record in-coming and out-going phone conversations.
- Calls to the main school office may be recorded for training purposes or in the event of an incident. Callers are made aware of this when they call the school.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Principal, School Business Manager and Online Learning Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working hours i.e. must be on a break
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students are present
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes
- Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).
- Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Online Safety policy.
- Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parent/carers could see them.
- Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.
- Staff must not use AI tools to process, analyse, or input personal or student data without authorisation from the Principal, School Business Manager, or Online Learning Manager.

5.2.1 Personal social media accounts

- Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.
- Members of staff must ensure that their personal use of social media is appropriate, professional, and consistent with the school's safeguarding responsibilities.
- Members of staff must not communicate with students or parents/carers via personal social-media accounts, or accept friend or follower requests from them. These expectations also apply after a student has left the school, for as long as there remains a potential professional relationship or safeguarding duty (for example, during the same academic year or while the individual is under 18).
- Posts, comments, and images must not bring the school into disrepute or compromise staff professionalism.
- Privacy and security settings on all social-media accounts should be reviewed regularly to ensure personal information is protected.
- The school provides guidance on appropriate privacy settings for social media accounts (see Appendix 1) and expects similar standards across other platforms.
- These expectations apply to all online activity, in or out of school, and operate alongside the Online Safety Policy and Staff Code of Conduct.

5.3 Remote access

- We allow staff to access the school's ICT facilities and materials remotely.
- Remote access is managed by the Online Learning Manager. We enable remote access via a secure VPN setup on school devices. VPN access from a personal device is not allowed unless approved by the Principal. To request remote access you must email the Principal or Online Learning Manager. Remote access may be withdrawn at any time at the discretion of the Principal.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Online Learning Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection policy.

Remote-access controls are reviewed annually as part of the school's online-safety and cyber-security risk assessment.

5.4 School social media accounts

The school's official social-media accounts (currently Facebook, X [formerly Twitter], Instagram and YouTube) are managed by the Principal and Online Learning Manager.

- Only authorised staff may access or post to these accounts. Other staff must not attempt to create, access, or manage official or unofficial accounts on behalf of the school.
- All content posted to official accounts must be professional, accurate, respectful, and consistent with the school's values, safeguarding responsibilities, and Data Protection Policy.
- Photographs, videos, or personal details of students must not be shared without the appropriate consent and in line with the Online Safety Policy and parental permissions.
- The Principal and Online Learning Manager reserve the right to edit or remove any posts that breach these standards or place the school at reputational or safeguarding risk.
- Authorised staff must follow the procedures set out in Appendix 2: Artificial Intelligence (AI) and Social Media - Guidance for Staff and ensure that all published content reflects the positive ethos and safeguarding standards of Voyage Learning Campus.

Breaches of these expectations may result in the removal of posting privileges and, where appropriate, disciplinary action.

5.5 Monitoring of school network and use of ICT facilities

The school monitors and logs ICT activity in line with the DfE Filtering and Monitoring Standards (2023) and relevant privacy legislation.

This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

The DSL and Online Learning Manager will jointly review filtering and monitoring logs termly, ensuring the systems meet DfE Filtering and Monitoring Standards (2023). Findings will be reported to the Management Committee annually.

Any safeguarding concerns identified through monitoring are logged in CPOMS and reviewed by the DSL and Online Learning Manager.

6. Students

6.1 Access to ICT facilities

- Students may access school computers and devices only under staff supervision or at designated times for self-study and approved school work.
- Each student will be provided with a unique school login to access computers, email, Microsoft 365 (Teams, OneDrive etc.) and other authorised apps.
- Students must keep their login details secure and must not share passwords with others.
- All activity on school systems is subject to the school's filtering and monitoring systems, which are reviewed regularly to keep students safe online in line with the DfE Filtering and Monitoring Standards (2023).
- Students must follow the principles set out in the Online Safety Policy and are expected to use ICT responsibly and respectfully at all times.

6.2 Search and deletion

- Under the Education Act 2011, and in line with the DfE guidance Searching, Screening and Confiscation (July 2022), the school may search students' phones, computers or other devices if there are reasonable grounds to believe they contain material that breaches school rules or the law (e.g. pornographic images, violent or extremist content).
- Any search will be conducted proportionately and with regard to safeguarding. The DSL will be informed of any material found that raises a safeguarding concern.
- Where appropriate, the school will follow the UKCIS Sharing nudes and semi-nudes: advice for education settings (2020) guidance.
- The school may delete files or data from a device if it is satisfied that the content has been, or could be, used to disrupt learning or break school rules.

7. Parents/Carers

7.1 Access to ICT facilities and materials

Parents and carers do not normally have access to the school's ICT facilities or systems. However, those working with the school in an official capacity (for example, as volunteers or on committees) may be granted limited access, such as to visitor Wi-Fi or online meeting platforms.

Any parent or carer who is granted such access must abide by this policy in the same way as staff and volunteers, particularly with regard to data protection and safeguarding.

7.2 Communicating with or about the school online

The school values positive relationships with parents and carers and encourages open, respectful communication. Parents and carers are expected to:

- Communicate courteously with staff and others in all online and digital interactions.
- Refrain from posting content online that could harm the reputation of the school, staff, or students, or that constitutes bullying, harassment, or defamation.
- Raise concerns or complaints through the school's official complaints procedure, rather than on social media.
- Support their children in using the internet safely and responsibly, following the principles set out in the Online Safety Policy.

The school may take appropriate action, in line with safeguarding and behaviour procedures, where online behaviour by a parent or carer is considered to pose a risk or cause harm to members of the school community.

8. Data security

All online safety incidents are logged through CPOMS in accordance with the school's safeguarding procedures.

Data protection incidents or data breaches are reported directly to the School Business Manager, who oversees investigation and reporting in line with the school's Data Protection Policy and Data Breach Procedure.

The school takes all reasonable steps to protect the security of its ICT systems, data and user accounts, in line with the DfE Meeting Digital and Technology Standards in Schools and Colleges (2024) and the NCSC Cyber Security Standards for Schools (2024). These controls include, but are not limited to:

- Firewalls and network-security features
- User authentication and multi-factor authentication (MFA)
- Anti-malware and endpoint-protection software
- Secure configuration of all devices and systems

While the school maintains robust technical and organisational safeguards, it cannot guarantee absolute security. All users of the school's ICT facilities - including staff, students, parents/carers, contractors and volunteers - must follow safe computing practices, use authorised systems only, and report any suspected data protection or cyber security incident immediately to the School Business Manager, or any online safety concern to the DSL.

The school continuously reviews its cyber-security arrangements through monitoring, audits and incident reporting to ensure ongoing compliance with DfE standards and safeguarding obligations.

8.1 Passwords

- **All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.**
- **Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.**
- **Members of staff or students who disclose account or password information may face disciplinary action.**
- **Parents/carers or volunteers who disclose account or password information may have their access rights revoked.**

8.2 Software updates, firewalls, and anti-virus software

- All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.
- Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
- Any personal devices authorised to connect to the school network must meet the same security standards, including regular updates and active anti-malware protection, as defined by the Online Learning Manager.

8.3 Data protection

- All personal data must be processed, stored and transferred in line with the UK GDPR, Data Protection Act 2018, and the school's Data Protection Policy.
- Any suspected or confirmed data breach must be reported immediately to the School Business Manager in accordance with the school's Data Breach Procedure.

8.4 Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
- These access rights are managed by the Online Learning Manager.
- Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Online Learning Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

- **The school ensures that its devices and systems have an appropriate level of encryption.**
- **School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the Principal.**
- **Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Online Learning Manager.**

9. Protection from cyber attacks

The school is committed to maintaining strong cyber-security defences to protect its systems, data, and users from attack or unauthorised access.

To achieve this, the school will:

- Work with the Management Committee, Senior Leadership Team and Online Learning Manager to ensure cyber security receives sufficient time, training and resources.
- Provide annual staff training (and induction for new starters) on identifying and reporting phishing, spoofing, and social-engineering attempts.
- Require all staff to check sender addresses carefully and verify any unusual requests for information or payments before responding.
- Maintain clear reporting procedures for suspected cyber incidents and respond promptly under the Data Breach Procedure and Business Continuity Plan.
- Review software and systems regularly to ensure they remain secure and supported, and avoid the use of obsolete or unpatched technology.
- Maintain multi-layered security controls, including firewalls, MFA, password managers, VPN access for remote users, and regular access-rights reviews.
- Back up critical data daily using cloud-based and/or offline storage solutions kept separate from the main network.
- Ensure backups are periodically tested to ensure data can be restored
- Conduct a cyber-security review or penetration test annually, and test its incident-response plan using the NCSC's Exercise in a Box or equivalent.
- Ensure all supply-chain partners and IT service providers follow secure practices, ideally holding Cyber Essentials or equivalent certification.

Any suspected cyber incident must be reported immediately to the School Business Manager and Online Learning Manager, who will coordinate the response and notify Action Fraud or external agencies where appropriate.

10. Internet access

The school's wireless internet connection is secured and monitored. All internet traffic is filtered in accordance with the DfE Filtering and Monitoring Standards (2023) and the school's privacy notice.

The Online Learning Manager and Designated Safeguarding Lead review filtering and monitoring systems annually to ensure they remain effective, age-appropriate, and proportionate to risk. In-year spot checks are carried out termly to confirm that alerts are functioning correctly.

On rare occasions, inappropriate content may not be filtered. Any such content must be reported immediately to the Online Learning Manager, who will investigate and, if a safeguarding concern is identified, ensure it is logged on CPOMS and reviewed by the DSL.

10.1 Students

Students are not permitted to use the school Wi-Fi except with the explicit permission of their teacher, and only for learning activities directly related to school work.

10.2 Parent/Carers and visitors

Parents/carers and visitors do not normally have access to the school Wi-Fi. The Principal may grant temporary access where it is necessary for the purpose of a visit (for example, to deliver a presentation or work in an official volunteer capacity).

The Principal will only grant authorisation if:

- Parent/carers are working with the school in an official capacity (e.g. as a volunteer)

- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not share Wi-Fi passwords or login details with anyone who is not authorised to have them.

Breaches of this rule may result in disciplinary action.

11. Monitoring and review

The Principal and Online Learning Manager are jointly responsible for monitoring the implementation and effectiveness of this policy.

They will ensure that:

- All staff, students and volunteers understand their responsibilities under this policy and receive regular reminders through training, briefings and updates.
- Filtering and monitoring systems are reviewed annually, and findings inform any required updates to this policy or the school's technical controls.
- The policy is reviewed every year, or sooner if significant changes occur in DfE guidance, legislation or school practice.

Any lessons learned from online safety incidents or cyber security reviews will be incorporated into future updates.

12. Related policies

This policy should be read alongside, and operates in conjunction with, the following school policies and procedures:

- Online Safety Policy
- Child Protection and Safeguarding Policy
- Relationships and Behaviour Policy
- Staff Disciplinary Policy
- Staff Code of Conduct
- Data Protection Policy
- Remote Learning Policy
- AI Usage Policy (to be adopted 2025/26)
- Business Continuity Plan

Together, these policies set out the school's comprehensive approach to safeguarding, data protection, and responsible use of technology.

Appendix 1: Social Media Privacy and Professional Conduct Guidance

This appendix provides guidance to help staff use social media safely, professionally, and in line with the school's **Staff Code of Conduct**, **Safeguarding Policy**, and the **ICT and Internet Acceptable Use Policy**.

A. Social-media privacy checklist

To protect your personal information and professional reputation, staff should:

1. **Review your privacy settings** regularly on all social-media accounts, see below.
2. **Restrict visibility** of your posts and photos to friends/followers only.
3. **Avoid sharing personal contact details**, addresses, or anything that could identify pupils or colleagues.
4. **Change your display name** use your first and middle name, use a maiden name, or put your surname backwards instead
5. **Check tagged photos** before approving them for public view.
6. **Do not post images** of students, colleagues, or the school environment without explicit permission and confirmation it aligns with the school's consent records.
7. **Turn off location sharing** and "check-in" features when posting.
8. **Use strong passwords and multi-factor authentication (MFA)** on all accounts.
9. **Keep personal and professional accounts separate**. Use official school channels for work-related communication.
    - Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
    - Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address / mobile number) is able to find you using this information.
10. **Think before you share**. Private posts can be copied, screenshotted, or shared by others.
11. **Report impersonation, hacking or misuse of school branding** to the Online Learning Manager immediately.

Check your privacy settings

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Google your name to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this
- Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

B. Professional conduct on social media

All staff must behave professionally online, just as they would in person.

1. Personal use

- Personal use of social media or messaging apps must not take place **during working hours** or **on school devices**, unless authorised for work purposes.
- Staff must not "friend", follow, or message students or parents/carers from personal accounts.

2. Referring to the school online

- Avoid naming or tagging **Voyage Learning Campus** or posting anything that could identify the school.

- Do not post or comment publicly about the school's operations, colleagues, students, or incidents.
- Do not discuss work-related matters, concerns, or frustrations on public platforms.
- Any professional reference to the school online must be respectful, factual, and approved by the Principal if it represents the school.

3. Acceptable online behaviour

- Apply the same standards of courtesy, confidentiality and professionalism online as you would at work.
- Do not post content that could be considered **offensive, discriminatory, defamatory, or incompatible with the school's values**.
- Avoid political or controversial statements that could be linked to your role at the school.
- Do not engage in online arguments or debates that may reflect negatively on you or the school.

C. Common pitfalls to avoid

Many online issues arise unintentionally. Staff should take particular care to avoid:

- **Posting in anger** - even without names, posts can be traced back or interpreted as unprofessional.
- **Assuming privacy** - private groups and direct messages can be shared by others.
- **Sharing workplace photos**- images of colleagues, students or classrooms must never be posted without permission.
- **Political or controversial content** - can be misinterpreted or linked to your professional role.
- **Identifying your workplace** - naming the school or listing it on your profile can connect your personal views to the school.

D. If you are contacted or harassed online

1. If a student adds or messages you

- Do not accept or reply.
- Block the student from viewing your profile.
- Notify the **DSL or OLM**, and record the concern on **CPOMS** if appropriate.
- If the student raises it in person, explain politely that staff cannot connect with students on social media.

2. If a parent/carer contacts you

- You may choose to ignore or politely decline.
- A neutral stock response is recommended (e.g. "I'm unable to connect via social media, but please contact the school office if you need to reach me.")
- Consider raising repeated or concerning contact with the Principal or DSL.

3. If you experience online harassment

- Do not respond or retaliate.
- Take screenshots or save the content as evidence (including time/date).
- Report the incident to the **Principal and OLM**, and to the **DSL** if safeguarding-related.
- The school will support reporting to platforms or the police where appropriate.

E. Support and reporting

Staff can seek advice about social-media concerns from the:

- **Online Learning Manager (OLM)** -technical and security issues
- **DSL** - safeguarding concerns
- **Principal** - professional conduct matters

Safeguarding-related incidents will be recorded on CPOMS.

Appendix 2: Artificial Intelligence (AI) and Social Media - Guidance for Staff

Purpose and scope

Artificial intelligence (AI) and social-media technologies are powerful tools that can enhance learning, communication, and professional collaboration. However, they also present safeguarding, data-protection, and reputational risks.

This appendix provides guidance for staff on their safe, ethical, and responsible use of AI and social media, in line with the school's Safeguarding, Online Safety, Data Protection, and Staff Code of Conduct policies.

1. Use of AI tools

- Staff must not input or upload personal or student data into AI tools when generating content for social-media posts or other public communications.
- AI-generated text, images, or videos must be reviewed carefully for accuracy and appropriateness before posting.
- Staff must not share or repost AI-generated content that could mislead, contain bias, or harm the school's reputation.
- Any use of AI to support communications must be transparent and in line with the school's Data Protection and Online Safety policies.
- Broader use of AI for teaching, learning, or administration is covered in the separate AI Usage Policy.

2. Social-media use

2.1 Approval and oversight

- The Principal and Online Learning Manager oversee all official Voyage Learning Campus social-media accounts (currently Facebook, X [Twitter], Instagram, and YouTube).
- Other staff may be granted posting access for specific purposes (e.g. sharing curriculum content or event updates) only with prior written approval from the Principal or Online Learning Manager.
- Any delegated access will be time-limited, role-specific, and reviewed regularly.
- The Online Learning Manager maintains a record of all authorised users and removes access immediately when staff move roles or leave.
- No staff member may create or operate an independent account representing the school without written approval.

2.2 Content principles

- Posts must be professional, accurate, respectful, and reflect the school's ethos and safeguarding responsibilities.
- Content must never include language or imagery that could be considered discriminatory, offensive, or inappropriate.
- Do not post photographs, videos, or personal details of students without appropriate consent and confirmation that sharing complies with the Data Protection Policy and parental-permission records.
- Avoid naming students in full or linking to their personal accounts.
- Ensure all content promotes a positive and inclusive image of Voyage Learning Campus.
- Avoid composing or uploading posts while supervising students, or at times when doing so could reduce attention to safeguarding or classroom-management responsibilities.

2.3 Security and access

- All official accounts must be protected by strong, unique passwords and multi-factor authentication (MFA) where available.
- Access must be from school devices or secure browsers only.
- Report any suspected compromise immediately to the Online Learning Manager, who will secure or suspend access.
- Passwords must be changed when staff with posting rights leave or roles change.

2.4 Moderation and response

- Respond to comments or messages only when appropriate and always in a professional manner.
- Do not engage in arguments, debates, or discussion of individual cases online.
- Report any abusive, defamatory, or safeguarding-related comments to the Online Learning Manager or DSL.
- The Principal and Online Learning Manager may edit, hide, or remove any post or comment that breaches these standards or risks the school's reputation or safeguarding responsibilities.

3. Compliance

- All use of AI and social-media tools must comply with:
  - Data Protection Act 2018 and UK GDPR
  - Keeping Children Safe in Education (KCSIE) 2025
  - DfE Filtering and Monitoring Standards (2023)
  - DfE "Using AI in Education" guidance (2025)
  - Online Safety, Safeguarding, and Staff Code of Conduct policies
- Breaches of this guidance may lead to the removal of posting rights and/or disciplinary action under the Staff Code of Conduct or Disciplinary Policy.