# Saffron Walden County High School

# Online Safety and Acceptable Use Policy

**Author:** Dan Wright (SAT ICT Hub Manager), Ben Johnson (SAT ICT Hub Manager)
**Date:** 1st October 2026
**Governor Approval Date:**
**Next Formal Governor Review:** October 2028
**Review Cycle:** The governing body will formally review and approve this policy every two years. The policy will also be checked and updated annually, and sooner where changes to guidance, technology, risks or school arrangements make this necessary.

## 1. Purpose, scope and principles

Saffron Walden County High School is committed to safeguarding and promoting the welfare of all students. Online safety is an essential part of safeguarding and is embedded within the school's culture, curriculum and everyday practice. This policy applies to everyone who uses the school's technology, accounts, networks, data or services, including students, staff, governors, volunteers, contractors, visitors, parents/carers and community users. It also applies to online behaviour outside school when it affects a student, a member of staff, the school community or the safe running of the school, including remote learning and the use of personal devices for school purposes.

The school takes a child-centred, whole-school approach that balances protection with the educational benefits of technology. The same standards of respect, safety and lawfulness apply online and offline. Risks are considered through content, contact, conduct and commerce, including emerging risks from artificial intelligence.

The school will help students use technology safely, responsibly and confidently. We will teach students how to recognise and report online risks, maintain appropriate filtering and monitoring, set clear expectations for acceptable use and provide additional support where a student has SEND or another vulnerability. Our approach will be reviewed in response to incidents, local needs, student feedback, changes in technology and national guidance.

## 2. Leadership and accountability

**Governing body and Headteacher**
The governing body approves and oversees this policy and receives assurance on safeguarding, curriculum and training. The safeguarding link governor provides designated oversight and reports relevant themes, concerns and actions to the governing body. The Headteacher is accountable for implementation, resources, staff conduct and effective cyber and data governance.

**Designated Safeguarding Lead (DSL) and SLT lead for online safety and safeguarding**
The DSL is the senior leader with overall responsibility for online safety and safeguarding. The DSL works with the Headteacher, the ICT Hub Manager, the nominated online-safety lead and other relevant staff to ensure that arrangements are understood and applied consistently. This includes overseeing filtering and monitoring, coordinating concerns and referrals, using local risks to inform the curriculum and reporting key themes to leaders and governors. Deputy DSLs support these responsibilities as delegated by the DSL.

**ICT Hub Manager / SAT Central ICT Team**
The ICT Hub Manager and SAT Central ICT Team implement secure systems, access controls, filtering, monitoring, updates, backups and incident response; record changes and checks; test protection before systems or devices are released; and work closely with the DSL.

**Curriculum leads and all users**
The Computing and PSHE/RSHE leads provide a planned, age-appropriate and inclusive programme. Staff follow this policy and the Staff Code of Conduct, supervise use, model professional behaviour and report concerns immediately. Students, parents/carers and other users follow the relevant expectations and cooperate with safeguarding action.

All staff must read and understand KCSIE 2026 Part One and any additional sections relevant to their responsibilities. Approvals and exceptions under this policy must identify the authorising

role, purpose, scope and duration. They must be recorded and reviewed when the need changes or the approval expires.

**Online-safety governance forum**

The school will maintain an online-safety group or equivalent governance forum that meets at least termly. Membership will include the Headteacher, DSL, safeguarding link governor, ICT Hub Manager or nominated SAT Central ICT Team representative, and other relevant staff as appropriate. The group will review online-safety incidents and trends, filtering and monitoring effectiveness, staff awareness and training, emerging risks and progress against agreed actions.

## 3. Education, training and engagement

Online safety is taught through RSHE/PSHE, Computing and relevant subjects. Teaching is sequenced, age-appropriate, adapted for SEND and vulnerability, and informed by statutory RSHE guidance, Teaching Online Safety in Schools and Education for a Connected World.

Teaching will help students understand privacy and security, consent and healthy relationships, respectful communication, cyberbullying, harassment, harmful sexual behaviour, grooming, exploitation, radicalisation, online hate, scams, misinformation, wellbeing, gaming, social media, image sharing, copyright, digital footprints and how to report concerns. Students will also learn about artificial intelligence, deepfakes and manipulated content. Pornography, misogyny and harmful online cultures will be addressed in an age-appropriate way. Sixth-form teaching will reflect students' increasing independence and their use of adult services, workplaces and higher-education settings.

Curriculum review, assessment, safeguarding information, student voice and staff feedback inform provision. Parents/carers receive accessible information through the website, communications, parents' evenings and other suitable activities, and may raise concerns with any member of staff or the DSL team.

Parents/carers confirm through Arbor that they have read this policy and will support its expectations. Students receive the requirements through induction and education; staff through induction and employment arrangements; and other users before access is provided where appropriate.

Staff and governors receive online-safety and filtering and monitoring training at induction, regular updates and role-specific training where required. Both groups use the Trust-provided usecure platform for cyber-security awareness, phishing simulations, password and data-protection training, and guidance on emerging threats. Governors also receive training through the school's wider governor training arrangements.

## 4. Reporting and responding to concerns

Anyone can report an online-safety concern to any member of staff. Staff must respond immediately, listen calmly, reassure the student, avoid blame, record the concern on CPOMS and pass it to the DSL without delay. Staff must not promise confidentiality or investigate beyond what is needed to keep the student safe. Students, parents/carers and staff must also have a clear way to report concerns when they are off site or the school is closed.

The DSL will assess the immediate and wider safeguarding risks, record decisions and decide what further action is needed. This may include involving parents/carers, early help, children's social care, the police, CEOP, Prevent, the local authority, the LADO or specialist services. The school will also respond to online incidents outside school where they affect safety, wellbeing, behaviour or the orderly running of the school. Concerns or allegations about an adult working with or around children, including low-level concerns, must be reported without delay through the route set out in the Child Protection and Safeguarding Policy. Concerns about the Headteacher must be reported to the Chair of Governors.

The school maintains a proportionate Prevent risk assessment and action plan informed by local risks, current guidance and relevant safeguarding information. The DSL ensures that staff understand the school's Prevent procedures and local referral routes. These arrangements are reviewed regularly and are read alongside the school's Child Protection and Safeguarding Policy.

### Sharing nudes and semi-nudes, intimate imagery and sexual extortion

Staff follow current UKCIS guidance and, unless specifically directed, must not view, copy, share, save or delete imagery, ask a student to share it, or search a device for it. The DSL completes the risk assessment and coordinates safeguarding and referrals. This includes AI-generated or manipulated imagery, nudification, non-consensual intimate imagery and financially motivated sexual extortion.

### Child-on-child abuse, bullying and harassment

Online bullying, sexual harassment, coercion, misogyny, hate, stalking, impersonation, threats and humiliating content are never dismissed as banter. The school considers patterns and power imbalance, supports affected students and addresses alleged harmful behaviour without prejudging the outcome.

### Illegal or harmful content

Suspected illegal material, terrorism, credible threats, exploitation or other crime must be escalated promptly. Staff must not investigate independently or circulate content; the DSL will seek advice and preserve evidence safely.

## 5. Filtering and monitoring

The school provides filtering and monitoring in line with the current DfE standard. The arrangements are appropriate to students' ages and the risks they may face. They aim to block harmful and illegal content without unnecessarily limiting teaching and learning. On systems that support it, protection can take account of text, images, audio, video and AI-generated content.

**The DSL** leads safeguarding decisions; the ICT Hub Manager implements technical controls; and the Headteacher and governing body provide oversight. Smoothwall provides filtering and

Impero Education Pro provides classroom management and safeguarding monitoring on supported school-managed devices. Detailed responsibilities, checks, review arrangements and outage procedures are set out in Appendix 4.

Authorised staff review alerts under documented procedures and escalate safeguarding concerns promptly. Urgent concerns are acted on immediately, and the DSL reviews reports and trends at least monthly. Operational checks occur at least half-termly and after material changes or incidents. The online-safety governance forum reviews incidents and trends, filtering and monitoring effectiveness, staff awareness and training, emerging risks and agreed actions at least termly. A documented strategic review takes place at least annually with safeguarding, technical, curriculum and governance input.

Staff must report gaps, overblocking, attempts to bypass controls or system failures to the SAT Central ICT Team. The DSL must also be informed where there is a safeguarding concern. Classroom supervision remains essential, and users must not try to bypass school controls. Any filtering change must be authorised, recorded, time-limited and reviewed. If filtering or monitoring is seriously affected, the SAT Central ICT Team will inform the DSL and Headteacher, assess the risk, put temporary safeguards in place and record when protection has been restored.

## 6. Acceptable use of technology, accounts and communications

School technology is provided mainly for learning and school business. Staff may make limited personal use where this is reasonable, lawful, secure and consistent with the Staff Code of Conduct. Users should understand that activity on school systems may be logged, monitored, inspected or disclosed where this is lawful and necessary.

Users must use only their authorised accounts, keep passwords and sign-in details private, use strong passwords and follow multi-factor authentication instructions. They must lock or sign out of devices when finished, protect devices and confidential information, use approved systems and communications, respect copyright and assessment rules, and follow staff instructions about games, streaming, shopping, social media, downloads and other non-learning activity. Harmful content, accidental access, malware, phishing, loss, theft, data breaches and security weaknesses must be reported immediately.

Users must not access, create, store or share illegal or harmful material; bully, harass, impersonate or exploit others; gain unauthorised access; damage systems; install unapproved software; bypass safeguards; use another person's account; or use school systems for commercial, unauthorised party-political campaigning or unlawful activity.

No new platform, application or service involving student login, communication, personal data or school content may be used without prior approval, appropriate risk and data-protection assessment, contractual safeguards and central administration.

## 7. Generative artificial intelligence

Artificial intelligence can support teaching, learning and school administration, but it must be used carefully. AI use must have a clear purpose, be appropriate for the user's age, be transparent and be supervised where necessary. Before a product is approved, the school will consider safeguarding, age suitability, SEND and accessibility, privacy, security, intellectual property, accuracy, bias and the need for human oversight.

Staff must not enter personal, special-category, safeguarding, assessment or confidential information into an unapproved AI service. They must check outputs for accuracy, bias, fabricated content, copyright and safeguarding risk. Students may use only authorised tools as directed, must acknowledge permitted assistance and must not cheat, impersonate, harass, create harmful or sexualised content, evade controls or disclose personal data.

Assessment use must follow current JCQ requirements and school procedures. AI-generated sexual or abusive imagery of a child is a serious safeguarding concern and may be illegal. Microsoft Copilot is currently the approved staff AI service, subject to Trust controls and review; students may use only specifically authorised services.

## 8. Personal devices, mobile phones and BYOD

The school is mobile-phone-free throughout the school day by default. Years 7–11 must keep devices switched off and stored as directed. Years 12 and 13 may use phones at lunchtime in designated sixth-form areas only as a formally approved exception to that default. The exception will be risk assessed, reviewed periodically and may be restricted or withdrawn where necessary. Phones must not be used in lessons, corridors or other restricted areas. A member of staff may authorise use for a specific educational, medical, accessibility or emergency purpose.

Students must not use personal devices to photograph, film, record or track another person without authorisation. Staff, governors, volunteers, contractors and visitors must not use a personal device to photograph, film, record or track pupils or school-related activities. Any exceptional adult use must be specifically authorised in advance, use approved safeguards and comply with safeguarding, information-governance, data-protection and cyber-security requirements. Personal devices must not be used to communicate during lessons or to bypass filtering through mobile data, hotspots, VPNs or proxies.

Where BYOD is permitted for Years 12 and 13, personal devices must connect through the school wireless network and follow the school's security, filtering and monitoring arrangements. Students are responsible for keeping their devices secure and charging them safely. Personal devices are brought to school at the owner's risk: the school does not insure or maintain them and cannot guarantee connectivity. BYOD access is mainly for learning and may be restricted or withdrawn if it is misused.

Years 7–11 may use a personal device only for an approved educational, medical or accessibility purpose. Educational use requires senior-leader authorisation, suitable controls, parent/carer permission where appropriate, use of the school network and staff supervision.

Searching, examination of data and confiscation will follow the school's behaviour and device-searching procedures and current DfE guidance. Any action must be authorised, proportionate and take account of safeguarding, privacy, equality and evidence preservation. Staff must not search for or view sexual imagery outside the UKCIS process.

## 9. Social media, images and professional boundaries

School communications must use approved channels. Staff and other adults must not connect privately with current students, follow student accounts, use personal messaging or discuss confidential matters online. Any pre-existing family connection must be declared and approved.

Official school or departmental social-media accounts must be approved, registered centrally and managed securely by at least two authorised members of staff. Accounts must be reviewed

regularly, and direct messaging with students is not permitted. Before posting or sharing content, staff must check that posts, links and reposts meet safeguarding, copyright, data-protection and professional standards. Online content must not bully, threaten or discriminate; disclose confidential or safeguarding information; damage professional boundaries; or bring the school or profession into disrepute.

Images and recordings of students require an authorised purpose, approved equipment or an authorised exception, relevant permissions and secure storage. Public content must not identify a student beyond what has been authorised. Copies must not be retained on personal devices or in personal cloud storage, including copies created automatically.

## 10. Data protection and cyber security

Users must comply with UK GDPR, the Data Protection Act 2018, school privacy information, retention requirements and DfE cyber-security standards. Necessary safeguarding information may be shared lawfully without consent to protect a child.

The school maintains proportionate access controls, secure configuration, patching, malware protection, backups, recovery, audit and incident arrangements. Cyber incidents, phishing, unauthorised disclosure, lost devices or compromised accounts must be reported immediately to the SAT Central ICT Team and, where relevant, the DPO and DSL. School devices remain subject to this policy off site; users must keep them secure, use approved software and services, and not store confidential information on unencrypted removable media.

## 11. Breaches, support and sanctions

The school will respond to misuse promptly, fairly and proportionately. Support and restorative action will be used where appropriate, alongside the school's safeguarding, behaviour, employment and disciplinary procedures. Depending on the circumstances, the school may restrict access, confiscate a device, require content to be removed, contact parents/carers, preserve evidence or make an external referral. Decisions will take account of age, SEND, vulnerability, intent, impact, repetition, coercion and the wider context.

Where access is restricted, the school will consider alternative supervised access so education can continue. Restrictions are reviewed and remain only while necessary and proportionate.

## 12. Monitoring, review and publication

The DSL keeps an overview of incidents and emerging online risks. The Headteacher ensures that leaders and governors evaluate implementation using evidence from training, curriculum delivery, filtering and monitoring, technical checks, incident trends, stakeholder feedback, cyber and data information, and audits. Review activity follows the operational, monthly, half-termly, termly and annual cycles set out in Sections 2 and 5 and Appendix 4. The policy owner will check and update the policy at least annually, and sooner where changes to guidance, technology, risks or school arrangements make this necessary. The governing body will formally review and approve the policy every two years and will receive appropriate assurance between formal reviews. The policy is published on the school website and included in induction and annual reminders.

## 13. Key guidance

This policy has been reviewed against the following guidance and standards. The policy owner must check these sources at least annually and whenever national guidance changes, and must update the policy or associated procedures where necessary.

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Filtering and monitoring core standard for schools and colleges
- Relationships education, relationships and sex education and health education: statutory guidance
- Generative AI product safety standards for educational settings
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- School inspection toolkit: operating guide and information

## Appendix 1: Student Acceptable Use Rules

School technology helps students learn, communicate and prepare for life beyond school. Students are expected to use school systems and personal devices safely, responsibly and respectfully. These rules follow the requirements in this policy and apply when students use school devices, accounts, networks or services, whether on or off site, and when they use a personal device for school purposes.

### My accounts and security

- I will use only my own authorised account and keep my password and sign-in details private.
- I will use strong passwords, follow multi-factor authentication instructions when appropriate and lock or sign out of a device when I have finished.
- I will protect devices and confidential information and will tell a member of staff straight away about accidental access, malware, phishing, loss, theft, data breaches or security weaknesses.
- I will not try to access another person's account, files or personal information.

### Respectful and responsible use

- I will communicate respectfully and will not bully, harass, threaten, impersonate, discriminate against, exploit or deliberately upset another person.
- I will not access, create, store or share illegal or harmful material, including abusive, sexual, extremist, hateful or humiliating content.
- I will respect copyright, licences, assessment rules and other people's work. I will not copy, alter or delete another person's files without permission.
- I will use school technology mainly for learning and school business and will follow staff instructions about games, streaming, shopping, social media, downloads and other non-learning activity.
- I will not damage or disrupt devices, networks or services, install unapproved software, gain unauthorised access, use another person's account, or use a VPN, proxy, hotspot or other method to bypass school controls.

### Approved systems and services

I will use only school-approved platforms, applications and services for school accounts, communication, personal data and school content.

### Privacy, communication and images

- I will protect personal and confidential information about myself and others and will share it only when authorised.
- I will use school-approved email, Teams or other approved services for school communication.
- I will not privately message staff through personal accounts or ask staff to connect with me on social media.
- I will not photograph, film, record, track or share information about another person without permission.
- I understand that anything shared online may be copied, changed or passed on and may be difficult to remove.

- I will not ask for, create, keep or share nude or sexual images, including AI-generated or manipulated images.

**AI, schoolwork and assessment**

- I will use only AI tools approved by the school and only in the way a member of staff allows.
- I will not enter personal, safeguarding or confidential information into an AI service.
- I will check AI-generated content carefully and will not assume that it is accurate, fair or suitable.
- I will acknowledge permitted AI assistance and will not use AI to cheat, plagiarise, impersonate someone, harass others or avoid assessment rules.

**Mobile phones and personal devices**

- If I am in Years 7–11, I will keep my phone switched off and stored as directed throughout the school day unless a specific exception has been authorised.
- If I am in Years 12 or 13, I will use my phone only at lunchtime in designated sixth-form areas where permitted. I will not use it in lessons, corridors or restricted areas unless authorised for a specific educational, medical, accessibility or emergency purpose.
- If BYOD is permitted, I will connect through the school wireless network, follow school security, filtering and monitoring arrangements and keep my device secure.
- I understand that personal devices are brought to school at the owner's risk. The school does not insure or maintain them and cannot guarantee connectivity.

**Reporting and help**

- I will report harmful content, suspicious messages, bullying, accidental access or anything that makes me or someone else feel unsafe to a member of staff as soon as possible.
- I will not forward harmful content or try to investigate it myself. I will not view, copy, share, save or delete nude or sexual imagery, ask another student to share it, or search a device for it.
- I know that I can report a concern to any member of staff, including when something happens outside school but affects the school community.

**Monitoring and consequences**

- I understand that activity on school systems and supported school-managed devices may be filtered, monitored, logged, inspected or disclosed where this is lawful and necessary for safeguarding, security and school operations.
- I understand that the school will respond to misuse promptly, fairly and proportionately. Depending on the circumstances, this may include support or restorative action, restricted access, confiscation of a device, removal of content, contact with parents/carers, preservation of evidence, disciplinary action or an external referral.
- I understand that decisions will take account of age, SEND, vulnerability, intent, impact, repetition, coercion and the wider context.
- If my access is restricted, I will follow any supervised alternative arrangements provided so that my education can continue.

Students and parents/carers confirm through Arbor that they have read and understood these rules and agree to support safe and responsible use of technology.

## Appendix 2: Staff, Governor, Volunteer and Visitor Acceptable Use Rules

These rules summarise the requirements for adult users and must be read alongside this policy and the SAT Code of Conduct, including its ICT Acceptable Use Policy. They supplement, but do not replace or weaken, those requirements. Where another applicable policy or procedure sets a stricter safeguarding, conduct, data-protection or security requirement, that stricter requirement applies.

**All adult users must**

- Use only their own authorised account, protect passwords and multi-factor authentication, lock unattended devices and report suspected compromise immediately.
- Use approved devices, software, applications, cloud services, AI tools and communication channels.
- Protect personal, safeguarding and confidential information, check recipients before sending and follow school retention and data-protection requirements.
- Communicate professionally, maintain appropriate boundaries and use school-managed channels for contact with students and parents/carers.
- Respect copyright, licences, intellectual property and assessment rules.
- Report harmful content, accidental access, phishing, malware, data breaches, loss, theft or security weaknesses without delay.

**Adult users must not**

- Access, create, store or share illegal or harmful material; bully, harass, impersonate or exploit another person; or use school systems for unlawful activity, commercial activity or unauthorised party-political campaigning.
- Share accounts, gain unauthorised access, install unapproved software, damage systems or bypass filtering and monitoring.
- Use personal accounts or messaging for school communications, connect privately with current students or discuss confidential school matters online.
- Store school data on personal devices or unencrypted removable media, or enter personal, safeguarding, assessment or confidential information into an unapproved AI service.
- Photograph, film or record students on a personal device or retain automatic personal cloud copies.

Limited staff personal use of school technology must be reasonable, lawful, secure and consistent with the Staff Code of Conduct. School-provided devices remain subject to these rules when used off site. Activity on school systems may be logged, monitored, inspected or disclosed where lawful and necessary.

Adults who receive access to school systems must confirm that they understand and will follow these expectations through induction, employment, governance, volunteering, contracting or visitor arrangements, as appropriate.

## Appendix 3: Mobile Phone and BYOD Rules

This appendix summarises the school's operational rules for mobile phones and personal devices. It should be read alongside Section 8, which sets out the policy principles, authorisation requirements and safeguards that apply to personal-device use.

**Years 7–11**

- Phones and similar devices must be switched off and stored as directed throughout the school day.
- A device may be used only for a specific authorised educational, medical, accessibility or emergency purpose.
- Planned educational use requires senior-leader approval, suitable safeguards, parent/carer permission where appropriate, connection through the school network and staff supervision.

**Years 12 and 13**

- Phones may be used at lunchtime in designated sixth-form areas where the school permits this.
- Phones must not be used in lessons, corridors or other restricted areas unless a member of staff has authorised a specific educational, medical, accessibility or emergency purpose.
- Where BYOD is permitted, devices must connect through the school wireless network and follow school security, filtering and monitoring arrangements.

**All personal devices**

- Devices must not be used to photograph, film, record or track another person without authorisation, communicate during lessons or bypass filtering through mobile data, hotspots, VPNs or proxies.
- Devices must be kept secure and charged safely. Personal devices are brought to school at the owner's risk; the school does not insure or maintain them and cannot guarantee connectivity.
- BYOD access is mainly for learning and may be restricted or withdrawn if it is misused. The school will consider alternative supervised access so education can continue.
- Urgent family messages must go through the school office.

**Adults**

- Staff must keep personal phones away during teaching and supervision except for an authorised purpose or emergency.
- Governors, volunteers, contractors and visitors must keep phones away when with students unless authorised and supervised.

Searching, examination of data and confiscation will follow current DfE guidance and the school's behaviour and device-searching procedures. Action must be authorised, proportionate and take account of safeguarding, privacy, equality and evidence preservation. Staff must not search for or view sexual imagery outside the UKCIS process.

## Appendix 4: Filtering and Monitoring Procedure

### Responsibilities

- The DSL leads safeguarding decisions, understands the systems and reviews relevant reports and trends.
- The ICT Hub Manager and SAT Central ICT Team configure, maintain and test technical controls, manage authorised changes and respond to failures.
- The Headteacher and governing body provide oversight and receive assurance that arrangements are effective.
- Authorised staff review Smoothwall and Impero Education Pro alerts under documented procedures and escalate safeguarding concerns promptly.

### Checks and review

- Operational checks take place at least half-termly and after material changes or relevant incidents.
- The DSL reviews reports, actions and trends at least monthly; urgent concerns are acted on immediately.
    - The online-safety governance forum reviews incidents and trends, filtering and monitoring effectiveness, staff awareness and training, emerging risks and agreed actions at least termly.
- A documented strategic review takes place at least annually and includes safeguarding, technical, curriculum and governance input.
- Reviews consider users, ages and needs, devices and locations, remote use, apps and AI-generated content, bypass methods, overblocking, alert thresholds, response times, records and effectiveness.

### Problems, changes and outages

- Staff must report gaps, overblocking, attempts to bypass controls or system failures to the SAT Central ICT Team. The DSL must also be informed where there is a safeguarding concern.
- Filtering changes must be authorised, recorded, time-limited where appropriate and reviewed.
- If filtering or monitoring is seriously affected, the SAT Central ICT Team informs the DSL and Headteacher, assesses the safeguarding risk, puts temporary safeguards in place and records restoration checks.

Classroom supervision and professional vigilance remain essential. Filtering and monitoring do not replace staff awareness or professional judgement.

## Appendix 5: Online-Safety Incident Procedure

### Immediate action

- Anyone may report a concern to any member of staff. Staff must respond immediately, listen calmly, reassure the student, avoid blame and explain that the concern must be shared.
- Staff must not promise confidentiality or investigate beyond what is needed to establish immediate safety.
- The concern must be recorded on CPOMS and passed to the DSL without delay. Immediate danger must be addressed through the school's emergency and safeguarding arrangements.

### DSL response

- Remove the approval assurance text completely
- The DSL assesses immediate and wider risk, considers context and vulnerability, records decisions and coordinates support and action.
- Action may include involving parents/carers, early help, children's social care, the police, CEOP, Prevent, the local authority, the LADO or specialist services.
- Incidents outside school are addressed where they affect safety, wellbeing, behaviour or the orderly running of the school.
- Concerns or allegations about an adult working with or around children, including low-level concerns, must be reported without delay through the route set out in the Child Protection and Safeguarding Policy. Concerns about the Headteacher must be reported to the Chair of Governors.

### Images, illegal content and evidence

- For nude or semi-nude imagery, including AI-generated or manipulated imagery, staff follow current UKCIS guidance. Unless specifically directed, they must not view, copy, share, save or delete imagery, ask a student to share it or search a device for it.
- Suspected illegal material, terrorism, credible threats, exploitation or other crime must be escalated promptly. Staff must not investigate independently or circulate harmful content.
- Evidence must be preserved safely, and decisions, referrals, actions and outcomes must be recorded.

### Follow-up

- The school supports affected students and responds to alleged harmful behaviour without prejudging the outcome.
- Responses are prompt, fair and proportionate and take account of age, SEND, vulnerability, intent, impact, repetition, coercion and context.
- Relevant themes inform the curriculum, training, filtering and monitoring, and the annual review.

## Appendix 6: Official Social-Media Account Rules

These rules apply to all official school, department, subject, club and activity accounts.

### Approval and account management

- Accounts must be approved before use, registered centrally and managed by at least two authorised members of staff.
- Access details must be held securely by the school, reviewed when staff roles change and removed promptly when access is no longer required.
- Accounts must use approved school contact details and settings and must be reviewed regularly. Unused accounts must be closed or archived securely.

### Communication and content

- Direct or private messaging with students is not permitted. Staff must not follow student accounts or use a personal account to manage school communications.
- Before posting, reposting or sharing links, images or video, staff must check the content, destination, audience, permissions and accessibility.
- Content must meet safeguarding, copyright, data-protection and professional standards and must not disclose confidential or safeguarding information.
- Posts must not bully, threaten or discriminate, damage professional boundaries or bring the school or profession into disrepute.

### Images and incidents

- Images or recordings of students may be used only for an authorised purpose after checking the school's permissions and safeguarding restrictions.
- Personal-device or automatic personal cloud copies must not be retained.
- Suspected compromise, harmful content, accidental disclosure or inappropriate contact must be reported immediately through the school's safeguarding, data-protection and cyber-security routes.