EF ACADEMY
International
Boarding Schools

OXFORD
E-SAFETY POLICY

This policy applies to the whole EF Academy Oxford community, on and off campus.

Document Owner	DSL
Document purpose	To set out how EF Academy Oxford protects and educates students and staff in their use of digital technology, identifies online risks, responds to concerns and meets its safeguarding responsibilities.
Scope	All students, including boarders and day students; all staff; governors/proprietor; volunteers; contractors; visitors; and any person using school systems, devices, networks or digital platforms.
Date Created	August 2026
Author	Deputy Head of School & DSL – Rob Tasker
Policy owner	Designated Safeguarding Lead (DSL), working with the Senior Leadership Team (SLT) and IT support.
Approval and oversight	The proprietor retains strategic oversight. The SLT is responsible for implementation and assurance. The DSL leads safeguarding and online safety. Named responsibilities must be recorded in the school's filtering and monitoring arrangements.
Review cycle	At least annually, and sooner following a serious incident, material change in technology, changes to the school's risk profile or updated statutory guidance.
Related school documents	Safeguarding and Child Protection Policy; Staff Code of Conduct; Student Handbook; Boarding Handbook / House Rules; Behaviour Policy; Anti-Bullying Policy; Child-on-Child Abuse procedures; Searching, Screening and Confiscation Policy; Mobile Phone / Personal Device rules; Data Protection and Records Retention Policy; Acceptable Use Agreements; Prevent Risk Assessment; Positive Mental Health and Wellbeing Policy; Complaints Policy; Whistleblowing Policy; Remote Education / Home Teaching and Learning guidance; Cybersecurity and Business Continuity procedures.
Wider documents used to support the development and review of this document	Keeping Children Safe in Education 2026; Education (Independent School Standards) Regulations 2014; National Minimum Standards for Boarding Schools; Working Together to Safeguard Children; DfE Filtering and Monitoring: Core Standard; DfE Cyber Security Standards; DfE Mobile Phones in Schools guidance; UKCIS Sharing nudes and semi-nudes advice (March 2024); relevant data protection legislation.
Last reviewed	September 2026
Review log	September 2026 – comprehensive revision to reflect KCSIE'26 September 2026, DfE digital and technology standards updated 16 September 2026, international boarding context, AI-related harms and updated operational responsibilities. September 2026 – Updated to reflect new SLT structure.
Date of next review	August 2027

1. Policy statement and principles

EF Academy Oxford recognises that digital technology is central to learning, communication, social life and the wellbeing of its international student community. For students living away from home, online communication is also an important way of maintaining relationships with family, friends and support networks across different countries and time zones.

The school will promote safe, responsible, respectful and informed use of technology. It will take a whole-school approach that protects and educates students and staff, and establishes effective arrangements to identify, intervene in, record and escalate online-safety concerns.

Safeguarding is everyone's responsibility. Online safety is not limited to school devices or the school day. Concerns arising through personal devices, social media, gaming, messaging services, AI applications or activity outside school must be considered where they may affect a student's safety, welfare, education or the school community.

- The welfare and best interests of children under 18 remain paramount.
- The school will take a child-centred, proportionate and non-judgemental approach, taking account of students' wishes and feelings.
- The school will recognise that students aged 18 and over are adults in law, while continuing to provide appropriate welfare support and taking action where their conduct or circumstances affect children, other students or the school community.
- The school will not assume that international students understand UK law, local support services, online norms or the risks of online contact in the same way. Information and education will be accessible to students for whom English is an additional language.
- Filtering and monitoring are important safeguards, but cannot replace education, supervision, professional curiosity, good relationships or prompt reporting.

2. Legal status, age and scope

KCSIE 2026 is statutory guidance in England and applies to safeguarding and promoting the welfare of children under 18. It must be read and followed by the school in carrying out its duties. The school's online-safety expectations apply to all students, including those aged 18 and 19, and to all members of the school community.

Where a student is aged 18 or over, staff must not automatically apply child-specific legal processes as if the student were under 18. The DSL should consider the adult student's welfare, capacity, consent, confidentiality and any relevant risk to a child or another person and obtain appropriate advice where necessary. Any concern involving a person under 18 must be managed through the school's child-protection procedures.

This policy applies:

- on school premises, in classrooms, offices, boarding houses and school transport;
- during school trips, educational visits, activities, work placements and events;
- to school-owned, personally owned and bring-your-own devices (BYOD);
- to school-managed networks, accounts, platforms and applications, and to personal online activity where it has a safeguarding or school-community connection;
- during evenings, weekends, holidays and periods when students are living away from campus, including online contact with peers, adults, guardians and family members.

The school may take reasonable and proportionate action in response to off-site or out-of-hours conduct where it affects the safety or wellbeing of a student, constitutes bullying or harassment, involves abuse or exploitation, disrupts school life, or creates a risk to the school community. Any action will be consistent with the Behaviour Policy, safeguarding procedures and applicable law.

3. Online-safety risks: the 4Cs

The school uses the four categories of online risk identified in KCSIE. These categories overlap and should be considered together.

CONTENT	Exposure to illegal, inappropriate or harmful material, including pornography; sexual or extreme violence; self-harm and suicide content; racist, misogynistic, antisemitic or other discriminatory material; radicalisation and extremism; misinformation, disinformation, fake news and conspiracy theories; harmful challenges; and AI-generated or manipulated material.
CONTACT	Harmful interaction with other users or AI applications, including grooming, coercion, exploitation, impersonation, adults posing as young people, peer pressure, harassment, stalking, controlling behaviour, financial or sexual extortion, and simulated relationships with AI chatbots.
CONDUCT	Behaviour that causes or increases the likelihood of harm, including cyberbullying, harassment, sharing or requesting nudes and semi-nudes, non-consensual image sharing, AI-generated sexual imagery or deepfakes, livestreaming, doxxing, impersonation, hate-based abuse, and accessing or distributing illegal material.
COMMERCE	Financial and commercial harms, including phishing, scams, identity theft, online gambling, in-game purchases, fraudulent investment or cryptocurrency schemes, money muling, blackmail, inappropriate advertising and exploitation for financial gain.

4. Roles and responsibilities

4.1 Proprietor / governance

- Retains overall strategic responsibility and seeks assurance that the school has effective online-safety, filtering, monitoring and cybersecurity arrangements.
- Ensures that a suitably senior member of the SLT and an appropriate proprietor/governance representative are identified as responsible for oversight.
- Receives regular assurance on the annual online-safety risk assessment, filtering and monitoring review, significant incidents, trends, actions and training.
- Ensures appropriate resources, systems, training and external technical support are available.

4.2 Senior Leadership Team

- Ensures this policy is implemented consistently and is reflected in the Safeguarding Policy and other relevant policies.
- Works with the DSL and IT support to define, document and review filtering and monitoring arrangements, including what is blocked or permitted and why.
- Ensures monitoring alerts and reports are assigned to trained staff, reviewed promptly and escalated appropriately.
- Ensures staff know how to report concerns, including out of hours and during boarding periods.
- Ensures the school's approach to mobile phones and personal devices is clear, consistently applied and appropriate to the school's day and boarding context.
- Ensures that online-safety education is embedded in the curriculum, induction, boarding programme and staff training.

4.3 Designated Safeguarding Lead

The DSL has lead responsibility for safeguarding and child protection, including online safety. The DSL must have appropriate authority, training, time and access to information to discharge the role.

- Leads the school's response to online safeguarding concerns and ensures that concerns are recorded on the school's safeguarding recording system.
- Understands the school's filtering and monitoring systems, their capabilities and limitations, and how to access and interpret relevant reports.
- Reviews or ensures review of safeguarding-related alerts and determines whether a concern requires immediate action, referral or wider risk assessment.
- Works with IT support and the SLT to review filtering and monitoring effectiveness and provides assurance to the proprietor/governance.
- Ensures incidents involving child-on-child abuse, sexual harassment, sexual violence, nudes and semi-nudes, grooming, exploitation, radicalisation or serious cyberbullying are managed under the relevant safeguarding procedures.
- Considers the views, wishes and feelings of the student, and involves parents/guardians where appropriate and safe to do so.
- Ensures relevant information is shared with the host local authority, placing authority (where applicable), police, children's social care, LADO or other agencies when required.
- Ensures online-safety training and student education reflect current risks, including AI and emerging technologies.

4.4 Deputy DSLs and boarding leadership

- Deputy DSLs act within the authority and arrangements delegated by the DSL and ensure that online-safety concerns arising during their duty periods are referred and recorded promptly.
- Boarding leaders and house staff maintain appropriate awareness of students' online welfare during evenings, weekends and overnight periods, without assuming that technical monitoring alone provides supervision.
- Boarding staff respond to disclosures, changes in behaviour, sleep disruption, distress, online conflict, unexplained gifts or money, secrecy, coercive relationships and concerns involving contact with unknown adults.
- Boarding staff must not investigate suspected abuse independently. They must preserve the student's immediate safety, report to the DSL/on-call safeguarding lead and follow the Safeguarding Policy.
- The school's boarding arrangements must make clear who is on duty, who can be contacted overnight and how urgent online-safety concerns are escalated.

4.5 IT support

- Maintains filtering and monitoring systems, access controls, network security, updates and technical logs in accordance with agreed responsibilities.
- Provides relevant reports and technical information to the DSL and authorised senior leaders in a timely manner.
- Works with the DSL and SLT to identify risks, test controls, investigate technical issues and complete documented reviews.
- Does not make safeguarding decisions independently. Where a technical alert may indicate harm, it must be escalated through the agreed safeguarding route.
- Ensures third-party providers understand their responsibilities, escalation routes, data protection obligations and service levels.

4.6 All staff, volunteers and contractors in regulated activity at the school

- Read and follow this policy, the Safeguarding and Child Protection Policy, Staff Code of Conduct and relevant acceptable-use rules.
- Complete online-safety safeguarding training at induction and receive updates at least annually, with additional updates when risks or systems change.
- Model safe, respectful and professional digital behaviour.
- Report concerns immediately to the DSL or a deputy; urgent or immediate danger must be escalated without delay.

- Do not promise confidentiality, investigate independently, confront a suspected perpetrator or view, copy, download or forward suspected illegal imagery.
- Remain alert to online elements in disclosures about bullying, mental health, sexual harassment, exploitation, radicalisation, discrimination and child-on-child abuse.

4.7 Students

- Use technology safely, respectfully, responsibly and lawfully.
- Follow the Student Acceptable Use Agreement (Appendix 1 of this policy), Mobile Phone / Personal Device rules and Boarding Handbook.
- Do not create, request, possess, forward or distribute abusive, humiliating, threatening or illegal material.
- Tell a trusted adult, the DSL, a deputy or another member of staff if something online makes them feel unsafe, pressured, upset or concerned about another person.
- Understand that asking for help will be treated seriously and supportively. Students will not be blamed for being targeted, groomed, coerced or exploited.

5. Filtering and monitoring

The school will maintain appropriate filtering and monitoring on school devices and school networks, in accordance with KCSIE 2026. Filtering is preventative: it seeks to block access to illegal, inappropriate or harmful content. Monitoring is reactive: it identifies or records activity and generates reports or alerts for review. Neither is a substitute for the other.

5.1 Responsibilities and decision-making

- The proprietor has overall strategic responsibility and must receive assurance that the standard is being met.
- The SLT, DSL and IT support work together. The DSL is named SLT lead and the named safeguarding lead for SLT (governance) representative will be recorded in the school's operational filtering and monitoring record.
- The DSL leads on safeguarding interpretation, reviews safeguarding alerts/reports and decides safeguarding action.
- IT support maintains the technical systems, provides reports, investigates technical faults and completes agreed technical actions.
- The school will document decisions about what is blocked or allowed and the rationale, including any exceptions for legitimate educational use.

5.2 Annual review and testing

The school will review its filtering and monitoring provision at least once in every academic year and sooner where a serious incident, change in technology, new AI product, change in student profile or identified weakness makes this necessary. The review will be undertaken by the SLT, DSL and IT support, with involvement from the responsible proprietor/governance representative.

- Identify the systems and devices covered, including school-owned devices, BYOD, Wi-Fi, mobile access and relevant cloud services.
- Check what is blocked and allowed, including illegal content, child sexual abuse material, terrorist content, pornography, self-harm, violence, gambling, proxy/VPN circumvention and other locally identified risks.
- Consider whether filtering and monitoring can identify or respond to dynamic, personalised and AI-generated content, and document limitations.
- Consider the age, maturity, needs, EAL profile and digital resilience of students, including those living in boarding accommodation.
- Review safeguarding incidents, alerts, false positives, missed risks, user reports, complaints and any known attempts to bypass controls.
- Test systems and escalation routes, record findings, assign actions, set deadlines and retain evidence for inspection.

The school will avoid unjustified over-blocking that prevents legitimate learning, research or access to support.

5.3 Monitoring alerts and escalation

- The school will maintain a written process identifying who receives alerts, who checks them, the expected response times, cover arrangements and how concerns are escalated outside normal school hours.
- Alerts suggesting immediate risk, exploitation, self-harm, threats, sexual abuse, terrorist content or serious harm must be escalated urgently to the DSL/on-call safeguarding lead.
- Alerts must be interpreted in context. A technical alert is not, by itself, proof of misconduct or abuse.
- Relevant alerts, decisions, actions and outcomes must be recorded securely, with access restricted to authorised staff.

5.4 Personal devices and limits

The school cannot guarantee that it can filter or monitor all activity on personal devices, mobile data connections, encrypted messaging services, private accounts or networks outside its control. Students and families must understand that school filtering may not apply when a personal device uses mobile data or another external network. This limitation does not reduce the school's responsibility to respond to safeguarding concerns brought to its attention.

6. Cybersecurity, accounts and personal information

- Staff and students must use individual accounts where provided and must not share passwords, authentication codes or access tokens.
- Passwords must be strong, unique and protected. Multi-factor authentication must be used where required by the school's systems.
- Users must lock devices when unattended, keep software updated and report lost or stolen devices, suspected account compromise or unusual activity immediately.
- Staff must not store school or student data in personal email accounts, unapproved cloud storage, personal messaging apps or unapproved AI tools.
- Personal data must be handled in accordance with the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025, together with the school's data protection and retention arrangements.
- Phishing emails, suspicious links, unexpected attachments, requests for gift cards or payments, impersonation and suspected scams must be reported to IT support using the school's designated reporting route.
- Any suspected data breach, unauthorised disclosure, loss of a device containing personal data or compromise of a school account must be reported immediately to the appropriate school data protection contact and IT support, as well as the DSL where student safety may be affected.
- The school will maintain proportionate cyber-security controls, backups, access management, supplier oversight and incident response arrangements.

7. Artificial intelligence and emerging technology

The school recognises that generative AI and other emerging technologies can support learning but can also create safeguarding, privacy, manipulation, misinformation, intellectual-property and wellbeing risks. This includes AI chatbots, image and video generators, voice cloning, deepfakes, automated translation, recommendation systems and immersive or virtual environments.

- Students may use only AI tools authorised or permitted by the school and must follow academic integrity requirements.
- Students must not enter personal, confidential, sensitive or identifying information about themselves or another person into an AI system unless specifically authorised for a legitimate educational purpose.
- Staff must not upload student data, safeguarding records, confidential school information or identifiable images to public or unapproved AI systems.
- AI-generated content must not be used to impersonate, threaten, humiliate, sexualise, exploit or harass another person.
- Creating, requesting, possessing or sharing AI-generated sexual images of a child, including deepfakes or deep nudes, must be treated as a serious safeguarding concern and referred to the DSL.
- Students must be taught that AI systems can produce inaccurate, biased or manipulative outputs and that simulated empathy or intimacy does not mean a chatbot is a safe or trustworthy person.

- The school will assess AI products before use, including their age suitability, safety features, data use, moderation, reporting tools, privacy settings and ability to expose students to harmful content.
- Staff must not rely solely on AI outputs for safeguarding decisions, risk assessments, disciplinary decisions or judgements about a student.

Where a student reports an AI-related incident, staff should preserve relevant contextual information (such as the platform, account name, date/time and URL where safe to do so) but must not download or circulate illegal imagery. The DSL will decide the appropriate safeguarding, technical and external referral response.

8. Mobile phones, personal devices and boarding arrangements

EF Academy Oxford is a 16–19 college. The school recognises that mobile phones and personal devices are an established part of students' everyday lives and that, given the age and maturity of its students, their use can support communication, independence, learning and the development of responsible digital citizenship.

Mobile phones are permitted on the EF Academy Oxford campus, including during the school day. However, students are expected to use them responsibly, respectfully and appropriately. Mobile phone use must not disrupt lessons, learning activities, meetings or other school activities, and staff may require phones to be put away or switched off where their use is inappropriate or interferes with teaching, learning, safety or the wellbeing and privacy of others.

Students must not use personal devices to:

- Photograph, film or record others without their knowledge or appropriate permission.
- Access, create, store or share inappropriate, harmful or illegal content.
- Bully, harass, intimidate or exploit another person.
- Share confidential information, personal data or images without permission.
- Circumvent the school's filtering, monitoring or other online safety arrangements.

The school expects students to exercise good judgement and take responsibility for their digital behaviour. Staff may impose reasonable restrictions on device use where necessary to maintain an appropriate learning environment or address a safeguarding, welfare or conduct concern.

For students living in school accommodation (See paragraph 8.1), these expectations apply equally within the boarding environment. Additional arrangements may apply to device use during study periods, supervised activities, overnight hours and other designated times. These are set out during induction and in the Student Acceptable User Agreement (Appendix 1 of this policy), Boarding Handbook or other relevant student guidance.

The detailed operational expectations, including permitted use, restrictions in lessons and activities, boarding arrangements, staff interventions, sanctions and any reasonable adjustments, are set out in the school's Student Acceptable User Agreement (Appendix 1 of this policy), Student Handbook and Boarding Handbook.

8.1 Boarding context

- Boarders may need access to devices outside the school day to contact parents, guardians and support networks overseas. Such access must be balanced with sleep, wellbeing, privacy, safeguarding and the rights of other boarders.
- Boarding house rules must specify permitted device use, quiet hours, overnight charging/storage expectations, use in shared areas, photography/recording restrictions and the response to misuse.
- Students must not photograph, film, livestream or audio-record another person in bedrooms, bathrooms, changing areas or other private spaces.
- Devices must not be used to intimidate, harass, bully, exploit, monitor, threaten or control another student or staff member.
- Staff must not impose blanket access to private messages or personal accounts. Any search or examination of a device must follow the Searching, Screening and Confiscation Policy.
- Where a student is distressed by online contact from home or overseas, staff should consider time-zone pressures, family dynamics, coercion, financial demands, threats and the student's ability to disengage safely.

- Where an online incident involves students in different countries, the DSL will consider the student's immediate safety in the UK, the need for UK referrals and any relevant overseas safeguarding or law-enforcement considerations. Staff must not attempt informal cross-border investigations.

8.2 Photography and recording

- No student or staff member may photograph, film, livestream or record another person without an appropriate lawful basis and the person's informed permission, except where an authorised school activity has been arranged under school procedures.
- Consent to being photographed does not permit the image to be edited, shared, posted or used for another purpose without appropriate authority.
- Images must never be taken in private spaces or used to ridicule, sexualise, threaten, harass, blackmail or control another person.
- Staff must use school-approved equipment and platforms for school photography and must follow consent, retention and publication procedures.

8.3 Staff use of devices

- Staff must not use personal devices to communicate privately with students or to store student images or personal data, except where an expressly authorised emergency or operational procedure applies.
- Digital communication with students must use approved school systems and remain professional, transparent and appropriate.
- Staff must not follow, friend or privately message students through personal social-media accounts.
- Staff must not use disappearing-message services for school communication.

9. Acceptable use and online conduct

9.1 General expectations

All users must use school technology and online services in a way that is safe, respectful, lawful and consistent with the school's values. Users must not:

- access, create, store or distribute illegal, pornographic, hateful, extremist, abusive or otherwise harmful material;
- bully, threaten, harass, stalk, intimidate, blackmail, groom, exploit or impersonate another person;
- share another person's personal information, images, location or private communications without proper authority;
- attempt to bypass filtering, monitoring, security controls or access restrictions, including through unauthorised VPNs, proxies or alternative accounts;
- access another person's account, files, messages or devices without permission;
- damage, disrupt or gain unauthorised access to school systems, networks or data;
- download or distribute malware, pirated material or unlicensed software, or engage in hacking, denial-of-service activity or other cybercrime;
- use school systems for gambling, scams, fraud, unauthorised commercial activity or other unlawful purposes;
- upload confidential or personal information to unapproved services or disclose passwords and authentication credentials;
- copy or use copyrighted material unlawfully or misrepresent another person's work as their own.

9.2 Email, messaging and social media

- Students must use school accounts for school business and must communicate respectfully.
- Staff must use approved school accounts and platforms for student communication. Communications must be professional, appropriate, capable of being audited and consistent with the Staff Code of Conduct.
- Students should use privacy settings, block and report abusive accounts, avoid sharing location information and think carefully before posting or forwarding content.
- Students must understand that content can be copied, altered, retained or redistributed even when an application describes it as private, temporary or disappearing.
- Staff must not use personal social-media accounts to engage with students or discuss confidential school matters.

9.3 Online relationships and exploitation

Staff should be alert to signs of grooming, coercion, trafficking, sexual exploitation, radicalisation, financial exploitation and controlling relationships. Indicators may include secrecy, sudden changes in online behaviour, unexplained gifts or money, threats, demands for images, pressure to move to encrypted platforms, contact with unknown adults, fear of losing access to an online relationship, or distress linked to a particular account or group.

Students should be taught that online relationships can involve people who misrepresent their identity or intentions. They should not meet an online contact in person without telling a trusted adult and following the school's safeguarding and off-site activity arrangements.

10. Child-on-child abuse, cyberbullying and harmful sexual behaviour

Online child-on-child abuse can take place on or off site and during or outside the school day. It may include bullying, discriminatory abuse, sexual harassment, sexual violence, coercive or controlling behaviour, threats, stalking, sharing images, hazing, initiation rituals and abuse through group chats or social media.

- All reports must be taken seriously and referred promptly to the DSL or a deputy.
- The school will not dismiss harmful behaviour as banter, drama, a joke, relationship conflict or a normal part of growing up.
- The DSL will assess the needs and safety of the victim, alleged perpetrator and other affected students, and consider immediate protective measures, support, referrals and the risk of retaliation or further sharing.
- The school will consider the impact on the wider boarding community, including rooming, house groupings, shared activities and contact outside school.
- Responses will be proportionate, child-centred and consistent with the Safeguarding Policy, Child-on-Child Abuse procedures, Anti-Bullying Policy and Behaviour Policy.
- Parents/guardians will normally be involved where appropriate and safe, taking account of the student's age, wishes, circumstances and any risk that parental involvement could increase harm.

Cyberbullying will be recorded and addressed under the Anti-Bullying and Behaviour Policies. The school may take action in relation to off-site activity where there is a sufficient connection to student safety, welfare or school life. The school will not promise that it can remove content from third-party services but may support reporting to the platform, the service provider or relevant authorities.

11. Sharing nudes and semi-nudes, deepfakes and sexual imagery

The school uses the term 'sharing nudes and semi-nudes' in line with UKCIS guidance. This includes images, videos or livestreams created or shared by a person under 18, whether self-generated, taken by another person, digitally altered or generated using AI. The term 'sexting' should not be used as the sole description because it may not reflect the nature of the incident.

Any incident involving the creation, request, possession, receipt or sharing of nudes or semi-nudes of a person under 18 must be referred to the DSL immediately and managed as a safeguarding concern.

11.1 Immediate staff response

1. Listen calmly, reassure the student that they have done the right thing by telling you, and do not blame or shame them.
2. Do not promise secrecy. Explain that information will be shared only with those who need to know to help keep people safe.
3. Do not view, copy, download, screenshot, print, forward or ask the student to send the image to you. Do not ask the student to show the image.
4. Do not ask the student to delete the image or message, or to forward it to another person. Do not undertake your own search of a device.
5. Record the disclosure in the student's own words, including relevant dates, platform/account details and immediate safety concerns, without reproducing the image.
6. Refer immediately to the DSL or deputy. If a child is at immediate risk of harm, follow emergency safeguarding procedures and contact the police/children's social care as directed.

The DSL will follow the current UKCIS guidance, assess whether the incident is experimental, consensual, coercive, abusive or adult-involved, consider whether there are multiple affected students, and decide on referrals to children's social care, police, CEOP or other agencies. The DSL will consider the need to inform parents/guardians unless doing so may increase risk.

11.2 AI-generated sexual imagery and sextortion

AI-generated or manipulated sexual images, including deepfakes and deep nudes, must be treated seriously even where the image is not a genuine photograph. Financially motivated sexual extortion (including threats to publish images unless money or further images are provided) must be escalated urgently. Staff should not negotiate with an extorter, make payment, or encourage the student to continue contact. The DSL will consider specialist police and CEOP advice.

11.3 Evidence and device handling

Any device or account that may contain evidence must be handled in accordance with the Searching, Screening and Confiscation Policy and police advice where appropriate. Staff must not conduct forensic searches, access private accounts or transfer imagery. Where a device is voluntarily shown, staff should avoid viewing the image itself and should seek DSL direction. If illegal imagery appears unexpectedly, stop viewing, do not copy or share it, and report immediately.

12. Other online safeguarding concerns

12.1 Self-harm, suicide and mental health

Online content may encourage self-harm, suicide, disordered eating, dangerous challenges or other harmful behaviour. Staff must respond to signs of distress, preoccupation with harmful content, threats or disclosures in accordance with the Safeguarding Policy and Mental Health and Wellbeing Policy. Any immediate risk of serious harm must be escalated urgently.

12.2 Radicalisation and extremism

Online material, encrypted groups, gaming platforms and social media may be used to promote extremist ideology, recruit or groom students, or encourage violence. Staff must report concerns to the DSL, who will follow the Prevent Risk Assessment and relevant referral procedures. Staff must not investigate suspected terrorist material or circulate it.

12.3 Misinformation and harmful online influence

Students will be supported to evaluate sources, recognise manipulated media and misinformation, understand algorithms and recommendation systems, and distinguish evidence from opinion. Staff should challenge harmful prejudice and conspiracy narratives in an age-appropriate and educational manner, while referring safeguarding concerns where a student appears to be targeted, radicalised or exploited.

12.4 Cybercrime and unsafe technical activity

Unauthorised access, hacking, malware, credential theft, denial-of-service activity, data theft or attempts to interfere with school systems must be reported to IT support and the DSL. Where a student demonstrates technical skills that may be developing into unlawful cyber activity, the DSL and SLT may consider a supportive early-intervention approach, including the National Crime Agency's Cyber Choices programme where appropriate.

13. Reporting, recording and responding

13.1 How to report

- Students may report to any trusted member of staff, the DSL, a deputy DSL, a house parent or another identified safeguarding contact on posters around the school.

- Staff must pass concerns to the DSL or deputy without delay and must not wait for proof or attempt to resolve the issue informally.
- Urgent concerns arising outside normal school hours must be reported through the boarding/on-call safeguarding arrangements.
- If a student or staff member is in immediate danger, contact emergency services as appropriate and notify the DSL/SLT as soon as possible.

13.2 Recording

- All online-safety and e-safety concerns must be recorded on the school's safeguarding recording form Safeguarding Concern Form Concerns or Disclosure August 2026.docx in accordance with the Safeguarding Policy and records-retention arrangements.
- Records should be factual, timely, proportionate and distinguish observed facts, the student's own words, third-party information and professional judgement.
- Record the platform/device where known, dates and times, people involved, immediate safety measures, advice received, referrals, decisions, rationale and follow-up actions.
- Where an incident involves bullying or child-on-child abuse, ensure records are linked appropriately to all relevant students without compromising confidentiality.
- Access to records must be restricted to those with a legitimate safeguarding or operational need.

13.3 Risk assessment and support

The DSL will assess immediate and ongoing risk, including risk of further contact, image circulation, retaliation, self-harm, exploitation, disruption to boarding arrangements and impact on other students. A risk assessment should identify protective actions, responsible staff, review dates and the student's support needs.

Support may include a trusted adult, pastoral or counselling support, a safety plan, changes to contact or living arrangements, help to report or remove harmful content, liaison with parents/guardians and referrals to external agencies. The school will consider the student's wishes and feelings and explain decisions wherever possible.

13.4 External referrals

The DSL will refer to children's social care and/or the police where the threshold is met, and will consult the local safeguarding partnership or relevant specialist services where needed. The school will follow local Oxfordshire safeguarding procedures and will consider the role of the host local authority and any placing authority. The school will contact the LADO where an online concern involves an adult working with children and may meet the relevant threshold.

Where a student is aged 18 or over, the DSL will consider the appropriate adult safeguarding, police, health or other referral route, while also assessing any risk to under-18s.

14. Searching, confiscation and access to devices

The school may search or confiscate a device only where there is a lawful basis and the action is authorised and carried out in accordance with the school's Searching, Screening and Confiscation Policy. This policy does not create a general power to search personal devices, compel disclosure of passwords, access private accounts or require students to delete material.

- Only staff authorised under the school's searching arrangements may conduct a search.
- Any search must be necessary, proportionate, appropriately authorised and recorded.
- Staff must not conduct an informal forensic examination or browse unrelated personal content.
- Where a device may contain evidence of a criminal offence or serious safeguarding incident, the DSL will consider police advice before further examination or handling.
- Staff must not delete, alter or destroy potential evidence. Any request to remove harmful content must be managed safely and must not compromise evidence or increase risk.
- Confiscated devices must be stored securely, access restricted and return arrangements documented.

The school will respect students' privacy and dignity and will consider reasonable adjustments and individual circumstances. Any action involving an adult student must also take account of their legal status and rights.

15. Photography, school publicity and student data

- The school will obtain and record appropriate permissions for the use of student photographs, video and other personal information in accordance with its data protection and communications procedures.
- Public-facing material should avoid publishing a student's full name alongside their image or information that could identify their location, routine or accommodation.
- Images must be appropriate to the activity and show students in suitable dress. Particular care must be taken with swimming, sports, changing and other activities where images may be misused.
- Staff must use approved school equipment and storage. Images must not be retained on personal devices or shared through personal accounts.
- Any concern about intrusive photography, unauthorised recording or misuse of images must be referred to the DSL.

16. Education, induction and training

Online-safety education will be age-appropriate, relevant to the school's 16–19 international student cohort and accessible to students with different levels of English. It will be delivered through curriculum teaching, induction, assemblies, boarding programmes, pastoral work and targeted support.

- Students will be taught about privacy, passwords, digital footprints, consent, respectful communication, cyberbullying, online relationships, grooming, exploitation, nudes and semi-nudes, sextortion, AI-generated imagery, misinformation, radicalisation, scams and how to report concerns.
- Students will be reminded that UK law applies to conduct in the UK, including online conduct, and that conduct may have consequences even if it takes place on an overseas platform or involves people in different countries.
- Boarders will receive specific guidance on online contact with family, guardians and agents, safe use of devices in residential accommodation, overnight routines, location sharing and what to do if online contact becomes threatening or coercive.
- All staff will receive online-safety safeguarding training at induction and regular updates at least annually. Training will include filtering and monitoring responsibilities, AI-related harms, image-sharing incidents, reporting routes and the limits of staff authority when handling devices.
- Parents and guardians will be provided with accessible information about the school's online-safety approach, monitoring arrangements, mobile phone expectations and how to raise concerns.
- The school will consider the need for targeted training for boarding staff, IT staff, DSLs, senior leaders, admissions staff and staff supervising trips or activities.

17. Parents, guardians and international context

The school recognises that parents and guardians may be based in different countries and time zones and may have different expectations, legal frameworks and cultural understandings of online activity. The school will communicate its expectations clearly and sensitively.

- Parents/guardians will be informed of the school's online-safety arrangements and relevant acceptable-use expectations.
- Where a safeguarding concern arises, the DSL will determine whether and when it is appropriate to contact parents/guardians, taking account of the student's age, wishes, safety and any risk that contact could increase harm.
- The school will not assume that an overseas guardian has parental responsibility or authority to receive confidential safeguarding information. This must be checked where relevant.
- Where a student is under 18, the school will follow child-protection information-sharing requirements and local safeguarding procedures.
- The school will provide students with information about UK-based support routes and emergency contacts, recognising that overseas family members may not be able to respond immediately.

18. Breaches, sanctions and support

A breach of this policy may result in action under the Behaviour Policy, Staff Code of Conduct, disciplinary procedures, safeguarding procedures or contractual arrangements. Responses will be proportionate and will take account of age, understanding, intent, impact, vulnerability, coercion, repetition and risk to others.

Possible responses include education and restorative work, support or safety planning, restrictions on access to school systems, supervised use, confiscation where lawful and authorised, parental/guardian involvement where appropriate, formal disciplinary action, suspension or exclusion in serious cases, referral to external agencies, or employment action for staff.

A student who has been targeted, coerced, groomed, exploited or pressured will be treated primarily as a person needing safeguarding and support. The school will distinguish victimisation from deliberate harmful conduct and will avoid responses that deter disclosure.

The school may report suspected criminal activity to the police. Staff must not promise that a matter will remain internal.

19. Review, audit and assurance

The school will carry out an annual review of its online-safety approach, supported by a documented risk assessment reflecting the risks faced by its students and staff. The review will consider:

- changes in student numbers, age profile, international composition, EAL needs and boarding arrangements;
- the 4Cs and emerging risks, including AI, deepfakes, chatbots, misinformation and financial sextortion;
- online-safety incidents, disclosures, bullying reports, safeguarding referrals and trends;
- filtering and monitoring capability, effectiveness, alerts, response arrangements and technical limitations;
- cybersecurity, account security, data protection and third-party platforms;
- student, staff, parent/guardian feedback and learning from incidents;
- the effectiveness of curriculum, induction, boarding education and staff training;
- the consistency of this policy with related policies and operational practice.

The review will produce a written record of findings, actions, owners and deadlines. The DSL will report significant risks and progress to the SLT and proprietor/governance. The policy will be updated sooner if required by changes in law, statutory guidance, technology or school practice.

Appendix 1 : STUDENT ACCEPTABLE USE AGREEMENT

Online safety, technology and digital behaviour | 2026–27

Student name	
Date / academic year	

This agreement applies to every student, including day students and boarders, and to school and personal devices when used in connection with school.

Why this agreement matters

Technology helps us learn, communicate with family and friends, and enjoy life at EF Academy Oxford. It also creates risks. We expect every student to use technology safely, respectfully, responsibly and lawfully.

These rules apply on campus, in lessons, in boarding houses, on school trips and activities, and outside school where online behaviour affects someone's safety, wellbeing or the school community. They apply to all students of all ages. Students under 18 are also protected by child safeguarding arrangements.

1. My everyday responsibilities

- I will use school devices, Wi-Fi, accounts, platforms and my own devices responsibly.
- I will follow staff instructions and the school's rules for phones, laptops, Wi-Fi, social media and boarding-house device use.
- I will treat other people online as I would expect to be treated face to face.
- I will think before I post, comment, share, forward, like or upload. Online content can be copied, saved and shared, even if an app says it will disappear.
- I understand that my online actions can affect other people and may have consequences under school rules and, in serious cases, the law.

2. Respect, kindness and online relationships

- I will not bully, threaten, harass, shame, intimidate, stalk, blackmail or impersonate anyone.
- I will not use group chats, gaming platforms, social media or messaging apps to target, exclude or humiliate another person.
- I will not share rumours, hateful content or discriminatory messages about someone's race, nationality, religion, sex, disability, sexuality or background.
- I will not pressure anyone to send images, reveal personal information, meet someone or do something they do not want to do.
- I will not use an online relationship to control, threaten or manipulate another person.

3. Photos, videos and private images

- I will not photograph, film, livestream or audio-record another person without appropriate permission.
- I will never take photos, videos or recordings in bedrooms, bathrooms, changing rooms or other private spaces.
- I will not post or share another person's image, video, voice recording or private message without their permission and, where required, the school's approval.
- I will never create, request, keep, send or share sexual images or videos of anyone under 18. This includes AI-generated, edited or deepfake images.
- I understand that forwarding an image can cause harm even if I did not create it.

If someone sends me a sexual image of a person under 18: I will not forward, screenshot, download, copy or show it to friends. I will not ask the person to send it again or ask them to delete it. I will tell the DSL, a deputy DSL or a trusted member of staff immediately.

4. AI, chatbots and deepfakes

- I will use only AI tools that the school allows and follow the school's academic integrity rules.
- I will not enter personal details, passwords, private messages, student information or confidential school information into an AI tool unless the school has specifically authorised it.
- I will not use AI to impersonate, sexualise, threaten, embarrass, bully or exploit anyone.
- I will not create or share fake sexual images, voice clones or videos of another person.
- I will remember that AI can make mistakes, give biased information and create convincing but false images, videos and messages. I will check important information and ask a trusted adult if I am unsure.
- I will not assume that an AI chatbot is a real person, a professional adviser or a safe place to share private information.
- I will use AI to support my learning, not to replace my own thinking or work. I will not present AI-generated content as my own.
- I will follow my teachers' instructions about when AI may be used, including for homework, assessments and coursework. Where AI use is permitted, I will acknowledge and reference it appropriately, in accordance with the school's Academic Integrity Policy and examination requirements.

5. Keep accounts, devices and information safe

- I will keep my passwords and verification codes private and will not use another person's account.
- I will use strong passwords, sign out when needed and lock my device when I leave it unattended.
- I will not click suspicious links, open unexpected attachments or respond to messages asking for passwords, money or personal details.
- I will tell IT support or a member of staff if my device is lost, my account may have been hacked, or I notice suspicious activity.
- I will not try to hack, damage, disrupt or gain unauthorised access to school systems, networks, accounts or data.
- I will not download or share malware, pirated material or unapproved software.
- I will not share my address, room number, travel plans, live location, passwords or private information with people I do not know and trust.

6. School systems, filtering and monitoring

- I understand that school devices and school networks are filtered and may be monitored to help protect students and the school community.
- I understand that filtering and monitoring may not cover every personal device, mobile data connection, private account or activity outside the school network.
- I will not try to bypass school filtering, monitoring or security controls, including by using unauthorised VPNs, proxies or alternative accounts.
- I understand that school systems should be used mainly for learning and other authorised school purposes.
- I will report harmful content, unsafe contact, bullying or suspicious activity rather than forwarding it or trying to investigate it myself.

7. Phones and devices in school and boarding

I will follow the school's Mobile Phone / Personal Device rules as outlined during school induction.

- I will only use my phone during lessons when a member of staff has authorised this.
- I will follow staff instructions about storing or putting away devices when needed.
- In boarding, I will follow boarding rules about device use, quiet hours, overnight routines and charging.
- I will not use devices to disturb other boarders' sleep, invade privacy or record people in private spaces.
- I understand that boarders may use devices to contact family and guardians, but this must be balanced with safety, respect, sleep and the wellbeing of others.

8. Social media, messaging and online contact

- I will use privacy settings and think carefully about who can see my posts and personal information.
- I will block and report accounts that threaten, harass, groom or pressure me.
- I will be careful if someone I have only met online asks to move to a private or encrypted chat, keep a relationship secret, send images, share money or meet in person.
- I will tell a trusted adult before arranging to meet someone I first met online.
- I will not use disappearing messages as a reason to send something unsafe or inappropriate.
- I will not use school accounts or networks for scams, gambling, fraud, blackmail or unauthorised commercial activity.

9. What should I do if something goes wrong?

You do not have to deal with an online problem alone. Tell someone as soon as possible, even if you are worried you may get into trouble or have made a mistake.

- Tell the DSL, a deputy DSL, your House Parent, a teacher or another trusted member of staff.
- If the concern happens at night or at the weekend, tell the boarding staff member on duty or use the school's on-call safeguarding arrangements.
- If you or someone else is in immediate danger, get help from a member of staff straight away and contact emergency services where necessary.
- Do not retaliate, threaten the other person, pay an extorter or continue a conversation that makes you feel unsafe.
- Do not delete or alter messages or other information that may help staff understand what happened. Ask staff for advice.
- If you receive or see a sexual image of someone under 18, do not copy, screenshot, download or forward it. Tell the DSL or a deputy immediately.

Asking for help is the right thing to do. The school will take concerns seriously and will aim to support students without blame or judgement. Staff may need to share information with people who can help keep someone safe.

10. What happens if I break these rules?

The school will consider what happened, the impact on others, the level of risk, your age and understanding, whether anyone was pressured or exploited, and whether the behaviour was repeated. Responses may include education, support, restrictions on access to school systems, device confiscation where authorised, parent/guardian contact where appropriate, or formal action under the Behaviour Policy. Serious concerns may be referred to external agencies or the police.

A student who has been bullied, groomed, pressured, coerced or exploited will be treated as someone who may need safeguarding support. The school will distinguish being targeted from deliberately causing harm.

Misuse of AI or other technology in academic work may also be investigated and addressed under the school's Academic Integrity Policy, including any applicable IB or A Level assessment regulations.

My agreement with the School

I have read this agreement, or had it explained to me in a language and way I understand. I know who I can speak to if I have a concern. I agree to follow these rules when using school technology and when my online behaviour affects the school community.

Student name (print)	
Student signature	
Date	

Staff member confirming discussion	

STOP • THINK • CHECK • REPORT

If you are worried, tell someone. You will be listened to.

Appendix 2 – Quick response guide for staff

If a student tells you about an online concern	Listen; reassure; do not blame; do not promise secrecy; establish immediate safety; record the student's words; refer to the DSL/deputy immediately.
If you encounter suspected nude/semi-nude imagery of a child	Do not view further, copy, screenshot, download, forward or ask to be sent the image. Do not ask the student to delete it. Stop and report immediately to the DSL.
If an alert suggests immediate danger	Escalate immediately to the DSL/on-call safeguarding lead and emergency services where necessary. Do not wait for routine reporting.
If you suspect grooming, sextortion or exploitation	Do not confront the suspected perpetrator or negotiate. Preserve non-image contextual details where safe. Refer immediately to the DSL.
If you suspect a cyber incident or data breach	Report immediately to IT support and the school's designated data protection contact; notify the DSL if student safety or safeguarding information may be affected.
If unsure	Report the concern. Staff do not need to prove that harm has occurred before raising a safeguarding concern.

Next review due: August 2027 (or earlier if required).

Appendix 3 – Key guidance and resources

- **Keeping Children Safe in Education 2026 (DfE, September 2026) –** https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- **DfE Filtering and Monitoring: Core Standard (updated 16 September 2026) –** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- **DfE Meeting Digital and Technology Standards in Schools and Colleges –** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- **UKCIS: Sharing nudes and semi-nudes – advice for education settings (updated March 2024) –** https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- **DfE: Generative AI in education and product safety standards –** https://www.gov.uk/government/publications/generative-ai-product-safety-standards
- **DfE: Safe use of generative AI in education – staff training –** https://www.gov.uk/government/publications/safe-use-of-generative-ai-in-education-module-3
- **National Minimum Standards for Boarding Schools –** https://www.gov.uk/government/publications/boarding-schools-national-minimum-standards
- **National Crime Agency – CEOP Education –** https://www.ceopeducation.co.uk/
- **National Cyber Security Centre – schools and colleges –** https://www.ncsc.gov.uk/section/education-skills
- **UK Safer Internet Centre –** https://saferinternet.org.uk/