

ONLINE SAFETY POLICY

Reaseheath College and University Centre

Designated Safeguarding Lead (DSL), with lead responsibility for online safety, filtering and monitoring	Laura Williams – Assistant Principal Student Experience and Support
Deputy Designated Safeguarding Leads / DSL Team Members	Paul Spearritt, Vice Principal Curriculum and Quality Kay Murray, Safeguarding Manager
Executive Lead for filtering and monitoring	Graeme Lavery, Vice Principal Finance and Resources
Safeguarding link governor	Mike Gorton
Curriculum leads with relevance to online safeguarding	James Eagney, Assistant Principal Performance and Progress Emily Jewell, Progress and Personal Development Manager
Network manager / other technical support	Gareth Ferris, IT Systems and Infrastructure Manager Phil Ball, ICT Operations Manager
Date this policy was reviewed and by whom	Approval as part of annual safeguarding and governance reporting in Term 1, 2026–27 Executive 09/09/2026
Date of next review and by whom	September 2027, or earlier if required – DSL / Assistant Principal Student Experience and Support

Introduction

What is this policy?

This policy brings together the College's strategic, safeguarding, educational, behavioural and technical arrangements for online safety. It is intended to remain a single comprehensive source of expectations and responsibilities, rather than relying on separate technical guidance to explain how online safety is managed.

Online safety is part of safeguarding. Concerns arising through technology must be considered with the same professional curiosity, urgency and care as concerns arising offline. Online and offline experiences frequently overlap, and online behaviour may be a cause, indicator or continuation of abuse, exploitation, harassment, bullying, radicalisation or other harm.

Who is it for; when is it reviewed?

The policy applies to all students, including children under 18 and adults, apprentices, higher education students, residential students, school pupils attending College activities, staff, governors, volunteers, contractors, agency staff, visitors and external users of College technology or premises.

The policy will be reviewed at least annually and sooner where there is a significant safeguarding incident, statutory or regulatory change, change to College technology, emerging risk, material change to filtering or monitoring, or learning from audit, complaints or quality assurance.

Who is in charge of online safety?

The Principal retains overall accountability. Laura Williams, Assistant Principal Student Experience and Support, is the Designated Safeguarding Lead and has lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. Graeme Lavery, Vice Principal Finance and Resources, is the Executive Lead for filtering and monitoring. In line with KCSIE 2026, the effectiveness of filtering and monitoring will be reviewed at least once every academic year. This review will be led by the Executive Lead for filtering and monitoring, with support from the DSL and IT support. Technical operation is undertaken by appropriately authorised IT staff. Governors provide strategic oversight and challenge.

What are the main online safety risks in 2026/2027?

The College considers risks through the four areas identified in Keeping Children Safe in Education 2026: content, contact, conduct and commerce. The College's assessment of risk also draws on local safeguarding intelligence, CPOMS records, filtering and monitoring alerts, student voice, residential context, curriculum need, SEND and high-needs provision, national reports and emerging trends. Online safety is therefore treated as part of contextual safeguarding, not simply as a technical matter.

Content: Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation, fake news, conspiracy theories, eating-disorder content and AI-generated harmful material.

Contact: Harmful interaction with other users or generative AI applications that simulate interaction, including peer pressure, grooming, coercion, adults posing as children, sexual or criminal exploitation, financial exploitation, harmful digital companions and manipulative or unsafe chatbot responses.

Conduct: Online behaviour that increases the likelihood of harm or causes harm, including cyberbullying, harassment, hate, impersonation, doxxing, livestreaming abuse, making or sharing nudes and semi-nudes, non-consensual image sharing, and digitally altered or AI-generated intimate imagery such as deepfakes or deep nudes.

Commerce: Online gambling, inappropriate advertising, phishing, scams, identity theft, fraudulent investment or cryptocurrency activity, in-game financial exploitation and financially motivated sexual extortion.

Particular attention will be given to students whose age, special educational needs or disabilities, communication needs, care experience, mental or physical health, residential status, experiences of abuse, social isolation or other circumstances may increase vulnerability or create barriers to recognising or reporting harm.

How will this policy be communicated?

- Published through the College's agreed policy channels and made available to staff, students, parents and carers.
- Included within staff induction, safeguarding training and regular updates.
- Reflected in student induction, personal development, curriculum activity and acceptable-use expectations.
- Explained to contractors, volunteers, visitors and external organisations where access to students, systems or premises creates an online-safety responsibility.
- Supported by accessible reporting routes and communications following significant changes.

Contents

Introduction	2
What is this policy?	2
Who is it for; when is it reviewed?	2
Who is in charge of online safety?	2
What are the main online safety risks in 2026/2027?	2
How will this policy be communicated?	3
Contents	4
Overview	6
Aims	6
Further Help and Support	6
Scope	6
Roles and responsibilities	6
Education and curriculum	6
Handling safeguarding concerns and incidents	7
Actions where there are concerns about a child	7
Nudes – sharing nudes and semi-nudes	7
Upskirting	7
Bullying	8
Child-on-child sexual violence and sexual harassment	8
Misuse of college technology (devices, systems, networks or platforms)	8
Social media incidents	8
CCTV	8
Extremism	8
Data protection and cybersecurity	8
Appropriate filtering and monitoring	9
Governance and annual review	9
Technical arrangements	9
Staff responsibilities for filtering and monitoring	10
Messaging/commenting systems (including email, learning platforms and more)	10
Authorised systems	10
Behaviour / usage principles of messaging/commenting systems	10
Use of generative AI	10
Online storage or learning platforms	11
College website	11
Digital images and video	11
Social media	11
Our social media presence	11
Staff, students' and parents' social media presence	11
Device usage	12
Personal devices including wearable technology and bring your own device (BYOD)	12
Use of college devices	12

Trips / events away from college	12
Searching and confiscation	12
Monitoring, quality assurance and review	12
Related policies and procedures	12
Legislation, statutory guidance and sector resources	13
Appendix – Roles	13
All staff	13
Principal	13
Designated Safeguarding Lead / Online Safety Lead	13
Governing Body, led by Online Safety / Safeguarding Link Governor	14
Personal Development Lead	14
Curriculum Area Managers and Tutors	14
IT Systems and Infrastructure Manager	14
Data Protection Officer (DPO)	14
Volunteers and contractors, including tutors	14
Students	15
Parents/carers	15
External groups	15
Document control and approval	15

Overview

Aims

- Safeguard students and promote their welfare online and offline.
- Enable safe, responsible, respectful, legal and purposeful use of technology.
- Develop digital resilience, critical thinking, media literacy and understanding of healthy online relationships.
- Ensure that roles, accountability and reporting routes are clear.
- Maintain proportionate, effective and regularly reviewed filtering and monitoring.
- Support appropriate innovation, including safeguarding-first use of generative AI.
- Protect personal data, College systems and the continuity of education.
- Respond consistently to incidents, preserve evidence and secure appropriate support.
- Ensure equality, accessibility and reasonable adjustments are considered in online-safety arrangements.

Further Help and Support

The DSL will maintain access to current statutory and sector guidance, including Department for Education, UK Council for Internet Safety, London Grid for Learning SafeguardED, Ofcom, National Cyber Security Centre, local safeguarding partnership and police guidance. External resources inform, but do not replace, professional judgement or College procedures.

Scope

This policy applies to College equipment, systems, accounts, networks, cloud services, communication platforms and data; personal devices connected to College Wi-Fi; College-managed devices used away from College; and online behaviour outside College where there is a safeguarding, conduct, employment, educational or reputational connection to the College community.

The policy covers fixed and mobile devices, wearable technology, cameras, microphones, smart devices, virtual and augmented reality, social media, gaming, messaging, livestreaming, online storage, educational technology, remote learning, artificial intelligence and future technologies with comparable functions.

Roles and responsibilities

Online safety is a shared responsibility. Detailed responsibilities are set out in the Appendix. No role description removes the duty of any person to act promptly if they become aware of a concern.

Education and curriculum

The College will provide a broad, age-appropriate and needs-informed approach to online-safety education. Curriculum and personal development activity will be sequenced and revisited rather than treated as a one-off event.

- How to evaluate online information, distinguish fact from opinion and recognise misinformation, disinformation, manipulated media and conspiracy narratives.
- Privacy, consent, healthy relationships, respectful communication and the implications of creating or sharing images.
- Cyberbullying, harassment, hate, radicalisation, exploitation, grooming, scams and financial harm.
- How algorithms, recommender systems, persuasive design and online advertising can shape attention and behaviour.
- Secure passwords, multi-factor authentication, phishing, malicious links, data protection and reporting cyber concerns.
- The opportunities and limitations of generative AI, including accuracy, bias, privacy, intellectual property, safeguarding and academic integrity.
- How to seek help, report concerns, block harmful contact and preserve evidence without forwarding illegal or harmful material.

Teaching will avoid unnecessarily exposing students to harmful content. Any planned use of sensitive material must have a clear educational purpose, appropriate risk assessment, suitable supervision and an alternative where reasonably required. Curriculum staff remain responsible for professional supervision even where technical controls are in place.

Handling safeguarding concerns and incidents

Any online concern involving a student must be considered under the College safeguarding framework. Staff must not promise confidentiality, conduct their own investigation, confront an alleged perpetrator, or ask a student to forward illegal imagery. Immediate danger or suspected crime must be escalated without delay.

1. Listen, remain calm and take the concern seriously.
2. Make an immediate safeguarding report using the College's approved recording route and contact the safeguarding team directly where urgency requires.
3. Record the student's words, the nature of the online service or device, relevant usernames or URLs where known, and action already taken. Do not copy or reproduce illegal imagery.
4. Preserve available evidence safely. Do not search a device or account beyond authorised powers and College procedure.
5. The DSL or deputy DSL will assess immediate safety, reporting, referral, parental engagement, police involvement, support, risk management and disciplinary considerations.
6. Separate safeguarding support from fact-finding and disciplinary processes so that welfare remains central.
7. Record decisions, rationale, actions, outcomes and review arrangements.

Immediate action

If there is an immediate risk to life or serious harm, contact emergency services and the safeguarding team without delay. If a member of staff may have harmed a student or behaved in a way that indicates risk, follow the allegations and low-level concerns procedures, not the student incident route.

Actions where there are concerns about a child

For students under 18, staff must follow the Child Protection and Safeguarding Policy and the current KCSIE 2026 action framework. The DSL will consider Family Help, statutory assessment, children's social care, police or other specialist referral according to the level and nature of risk. Where a child is suffering or likely to suffer harm, referral must not be delayed.

Where the concern relates to an adult student who may have care and support needs and may be experiencing or at risk of abuse or neglect, the Safeguarding Adults Policy and relevant local adult safeguarding arrangements will apply.

Nudes – sharing nudes and semi-nudes

For this policy, nudes and semi-nudes include photographs, videos, livestreams and all other visual content. Images may be taken by a child or another person, digitally altered, or wholly or partly generated using artificial intelligence, including deepfakes and deep nudes. A concern remains serious even where the image does not depict an event that occurred in reality.

- Staff must report immediately to the DSL and must not view, copy, print, save, forward or ask a student to send the image, unless exceptional viewing is authorised and necessary under current UKCIS (UK Council for Internet Safety) guidance.
- Staff must not delete material before advice is obtained where deletion could impede safeguarding or law-enforcement action.
- The DSL will complete a proportionate risk assessment considering age, consent, coercion, distribution, vulnerability, adult involvement, commercial motives, threats, blackmail, recurrence and immediate safety.
- The College will provide support to the person depicted and consider risk and support in relation to other involved students.
- Incidents involving financially motivated sexual extortion, adult involvement, coercion, blackmail, significant age difference, trafficking, or distribution for gain require urgent specialist and police consideration.

Upskirting

Upskirting is a criminal offence and a form of sexual abuse. Any concern that an image has been taken under a person's clothing without consent for sexual gratification or to cause humiliation, distress or alarm

must be reported immediately. This includes attempted acts and the sharing or threatened sharing of resulting material.

Bullying

Cyberbullying will be addressed under safeguarding, student conduct and harassment and bullying arrangements. The College recognises that online bullying can be continuous, rapidly amplified, anonymous, permanent or difficult to escape. Harm may occur through messages, images, exclusion, rumours, impersonation, gaming, group chats, livestreams, location sharing or coordinated attacks.

Child-on-child sexual violence and sexual harassment

The College adopts a zero-tolerance approach. Online sexual harassment may include unwanted sexual comments, sexualised bullying, sharing sexual content, coercing image creation, threatening disclosure, rating appearance, sexualised deepfakes, or persistent contact. Reports will never be dismissed as banter, part of growing up or an inevitable part of online life.

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

Misuse may lead to safeguarding action, restriction of access, disciplinary action, recovery of loss, referral to an awarding body, employer, police or regulator, and other proportionate action. The response will consider intent, impact, age, capacity, vulnerability, repetition, prior education and whether the person may also have been exploited or harmed.

- Attempting to access, create, possess or distribute illegal or harmful material.
- Bypassing or attempting to bypass filtering, monitoring, security, account controls or licence restrictions.
- Using another person's account, sharing credentials or interfering with systems or data.
- Malware, phishing, hacking, denial-of-service activity or unauthorised scanning.
- Harassment, threats, hate, impersonation, fraud, deceptive AI content or unauthorised recording.
- Using College systems for unlawful commercial activity, gambling, extremist activity or sexual exploitation.

Social media incidents

Where social-media activity affects safety, wellbeing, learning, employment or the orderly operation of the College, the College may act even if the activity occurred away from College or on a personal account. Staff should capture available reporting information without unnecessarily reproducing harmful content and refer the matter promptly.

CCTV

CCTV and other security footage will be used only in accordance with College policy, data protection laws and authorised purposes. Access, disclosure, retention and evidential use must be controlled. CCTV must not be used as a substitute for appropriate supervision or safeguarding action.

Extremism

Online radicalisation may occur through social media, gaming, encrypted messaging, video platforms, forums, influencers, manipulated media and generative AI. Staff must report concerns under the Prevent and safeguarding arrangements. Filtering supports, but cannot replace, education, professional curiosity, relationships and proportionate referral.

Data protection and cybersecurity

The College will comply with data protection laws, including the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with other applicable law and College policy. The Data (Use and Access) Act 2025 amends and builds on the existing UK GDPR, Data Protection Act and Privacy and Electronic Communications framework; it does not replace the need for lawful, fair, transparent and secure processing. Appropriate information sharing for safeguarding is not prevented by data protection law, and fears about sharing information must not stand in the way of protecting a child or adult at risk.

- Personal data must be processed through authorised systems, accessed only where required and shared securely.

- Sensitive, confidential, personal, safeguarding or commercially restricted information must not be entered into unapproved AI, messaging, storage or transcription services.
- Users must protect credentials, use multi-factor authentication where required, lock devices, install updates and report loss, compromise or suspicious activity promptly.
- Phishing, malicious links, malware, ransomware, account compromise and data loss may create safeguarding as well as operational risks and must be escalated accordingly.
- The College will maintain proportionate backup, recovery, access-control, logging, incident-response and business-continuity arrangements.
- Cyber incidents involving student welfare, records, location, identity, communication or vulnerable individuals will be jointly considered by IT, the DPO and safeguarding leads.

Appropriate filtering and monitoring

The College will do all that it reasonably can to limit students' exposure to online risks through its IT systems while avoiding unreasonable overblocking that restricts education, inclusion or access to support. Filtering and monitoring form part of a wider safeguarding system and do not replace staff supervision, education, behaviour expectations or professional judgement.

Governance and annual review

The Governing Body will ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year. The review will be led by Graeme Lavery, Vice Principal Finance and Resources and Executive Lead for filtering and monitoring, with the support of the DSL and IT support.

- The review will be documented and will identify the systems in use, ownership, scope, limitations, risks, testing undertaken, findings, decisions, actions, responsible persons and completion dates.
- Checks will cover College-managed internet-connected devices and relevant locations, remote use where applicable, personal devices on College Wi-Fi, College accounts and cloud services within the capability of the approved systems.
- Testing will consider different user groups, age and vulnerability, safeguarding categories, search and video settings, encrypted traffic, mobile data, personal hotspots, VPNs, browser extensions, applications and other foreseeable routes around controls.
- The College will consider both underblocking and overblocking, including whether students can access legitimate curriculum, health, safeguarding and support information.
- Significant findings and unresolved risks will be reported through safeguarding and governance arrangements.

Technical arrangements

The College currently uses centrally managed filtering and monitoring controls, including Cisco Umbrella and Lightspeed Alert / Human Review, together with Microsoft 365 and network controls where configured. These arrangements support, but do not replace, staff vigilance and safeguarding practice. IT Services must confirm product names, licensing, coverage, alert pathways, monitoring of student and staff accounts where applicable, data processing, out-of-hours arrangements and known limitations as part of the annual review and whenever material changes are made.

- Internet access will be filtered according to role and educational need, with changes authorised and recorded.
- Monitoring alerts will be triaged by authorised personnel using agreed thresholds and escalation routes.
- The DSL must understand what is filtered and monitored, how concerns are escalated, expected response arrangements and known limitations.
- Technical staff with access to monitoring information must receive safeguarding, confidentiality and escalation training appropriate to their role.
- Change-control records, test evidence, alert outcomes and review evidence will be retained in line with College retention arrangements.
- No monitoring system will be represented as comprehensive. Students and staff will be informed that use of College systems may be filtered, logged and monitored in accordance with law and policy.

- Records of filtering and monitoring checks will be retained, including when checks were carried out, which systems, devices, locations and user groups were tested, issues identified, decisions made and actions completed.

Staff responsibilities for filtering and monitoring

- Maintain appropriate physical supervision and do not assume blocked content cannot be accessed.
- Report sites or services that should be blocked, legitimate material that is wrongly blocked, suspected circumvention and monitoring failures.
- Act on concerning behaviour or disclosures even where no automated alert is generated.
- Do not attempt to test filtering using illegal search terms or imagery. Approved test plans must be used by authorised staff.
- Use approved accounts, devices and communication services for College business.

Messaging/commenting systems (including email, learning platforms and more)

Authorised systems

College business and communication with students must take place through authorised systems and accounts. Personal email, personal messaging accounts and disappearing-message services must not be used for routine staff-to-student communication. Exceptions require explicit authorisation, a recorded rationale and suitable safeguards.

Behaviour / usage principles of messaging/commenting systems

- Use professional, respectful and unambiguous language.
- Maintain appropriate boundaries and avoid unnecessary private or late-night communication.
- Use group or transparent communication where appropriate and retain auditable records.
- Do not share personal contact details unless authorised for a defined operational purpose.
- Check recipients, attachments, permissions and sensitivity before sending.
- Report misdirected, harmful, threatening or suspicious messages promptly.
- Do not use College systems to bully, harass, discriminate, intimidate, groom, radicalise, defraud or distribute illegal or inappropriate material.

Use of generative AI

The College supports responsible use of approved generative AI where it has a legitimate educational or business purpose. A safeguarding-first approach will be applied to selection, configuration and use. Approval must consider age restrictions, privacy, security, intellectual property, accessibility, bias, moderation, accuracy, data retention, use of prompts for training, human oversight, safeguarding escalation, dynamic generated content and compatibility with filtering and monitoring.

- Users must follow College and awarding-body requirements concerning acknowledgement, authorship, assessment and academic integrity.
- AI output must be checked by a competent person. It must not be treated as factual, neutral, safe or complete without verification.
- Users must not create or distribute sexual, abusive, discriminatory, deceptive, threatening or humiliating content, including deepfakes or deep nudes.
- Students must not be directed to use an AI service unless it has been approved and the activity is suitable for their age and needs.
- AI must not make final safeguarding, disciplinary, admissions, assessment, employment or other high-impact decisions without authorised human judgement.
- Staff must report harmful output, unsafe interactions, data disclosure, suspected grooming or manipulation, and misuse that creates risk.
- AI companions, simulated relationships and therapy-style bots can create contact and dependency risks. They must not be presented as substitutes for professional support.
- Staff must not upload identifiable student images, safeguarding records or confidential College information to unapproved AI tools, including image, video, voice, transcription, meeting-summary or note-taking services.

Online storage or learning platforms

Only approved storage and learning platforms may be used for College information and learning activity. Access must be role-based, reviewed, removed promptly when no longer required and configured to prevent inappropriate public sharing. Staff must check sharing permissions and avoid storing safeguarding records outside approved case-management arrangements.

College website

Published content must be accurate, accessible, lawful and approved. Personal information and images must be used consistently with privacy notices, permissions and safeguarding considerations. Contact details should support College communication without unnecessarily exposing personal staff information. Website forms, accounts and plug-ins must be maintained securely.

Digital images and video

- Images or recordings must have a legitimate purpose and be captured, stored, used and deleted through authorised arrangements.
- Consent and lawful basis must be considered, together with safeguarding, dignity, cultural, location and identification risks.
- Personal devices must not be used to photograph or record students for College purposes unless an authorised exception and secure transfer process are in place.
- Recording is prohibited in toilets, changing areas, bedrooms and other private spaces except where expressly lawful and authorised for a specific safeguarding or investigative purpose.
- Staff must not publish student images through personal accounts.
- AI editing, facial manipulation, voice cloning and synthetic media must not be used in a way that misrepresents, humiliates or harms any person.
- Particular care will be taken before publishing images that could be copied, manipulated or repurposed using AI. The College will consider whether image use creates additional risk because of vulnerability, residential status, safeguarding history, location information or the ease with which faces or voices could be extracted.

Social media

Our social media presence

Official social-media accounts must be authorised, assigned to named staff, protected by appropriate access controls, moderated and reviewed. Account ownership must remain with the College. Content and responses must protect safeguarding, confidentiality, copyright, accessibility, reputation and data protection.

Staff, students' and parents' social media presence

- Staff must maintain professional boundaries and must not use personal social-media accounts to establish or pursue inappropriate relationships with students.
- Staff must not discuss confidential College, staff or student matters through personal accounts.
- Students and parents or carers are expected to raise concerns through appropriate College channels and not use social media to harass, identify or target individuals.
- The College respects lawful private expression but may act where online conduct creates safeguarding risk, breaches policy, undermines professional standards or significantly affects the College community.
- Safeguarding concerns must not be investigated through personal social-media searches unless authorised, necessary, proportionate and lawful.

Device usage

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

Personal devices are permitted subject to reasonable restrictions, curriculum direction, safeguarding, security and conduct requirements. The College recognises that mobile data, hotspots and unmanaged applications may sit outside College filtering. Staff supervision and education therefore remain essential.

- Devices must be silent and stored during teaching or assessment unless use is authorised.
- Photography, audio or video recording, livestreaming and location sharing require permission and must respect privacy and safety.
- Personal hotspots, VPNs or other methods must not be used to bypass College controls.
- Wearable devices, smart glasses and AI-enabled recording tools are subject to the same expectations as phones and cameras.
- Reasonable adjustments, medical use, accessibility and emergency communication will be considered proportionately.
- The College is not responsible for loss or damage except where legal liability applies.

Use of college devices

- College devices must be used primarily for authorised education or work.
- Users must not disable security, install unauthorised software, connect unapproved hardware or allow another person to use an authenticated session.
- Devices must be kept secure, returned when requested and reported immediately if lost, stolen or compromised.
- College-managed devices remain subject to management, filtering, logging and monitoring wherever the configured systems operate.

Trips / events away from college

Risk assessments for trips, placements, fieldwork, competitions, residential activity and events must consider connectivity, staff communication, photography, social media, location sharing, emergency contact, device charging, accommodation privacy and access to harmful content. College expectations continue to apply off site and abroad, subject to local law and practical limitations.

Searching and confiscation

Searching, screening and confiscation will be undertaken only by authorised staff in accordance with law and College policy. Staff must consider whether a device may contain illegal imagery or evidence and seek DSL or police advice before viewing content. Any action must be necessary, proportionate, recorded and respectful of privacy and dignity.

Monitoring, quality assurance and review

The College will complete an annual review of its whole-college approach to online safety, supported by an online-safety risk assessment reflecting the risks faced by its student population.

- Safeguarding incident themes and outcomes.
- Filtering and monitoring review evidence, alerts, failures, change requests and overblocking.
- Student, staff and parent or carer voice where appropriate.
- Curriculum coverage, staff confidence and training needs.
- Generative AI, social media, cyber security and emerging technology risks.
- Equality, SEND, accessibility, residential and other contextual considerations.
- Complaints, whistleblowing, data incidents, audit findings and lessons learned.
- Actions, owners, deadlines and evidence of completion.

The DSL will provide anonymised assurance information through the College's safeguarding governance arrangements. The Governing Body will test whether arrangements are understood, effective, proportionate and sufficiently resourced.

Related policies and procedures

- Child Protection and Safeguarding Policy
- Safeguarding Adults Policy

- Student Conduct Policy
- Student Harassment and Bullying Policy and Procedure
- Staff Code of Conduct
- Acceptable Use requirements
- Social Media policies
- Data Protection Policy and privacy notices
- Information Security and Cyber Security arrangements
- Prevent risk assessment and action plan
- Academic integrity and assessment malpractice arrangements
- Residential safeguarding and behaviour procedures
- Whistleblowing, complaints and allegations procedures

Legislation, statutory guidance and sector resources

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children
- Prevent Duty Guidance
- Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025
- Equality Act 2010 and Human Rights Act 1998
- Voyeurism (Offences) Act 2019 and applicable sexual offences legislation
- Department for Education filtering and monitoring standards for schools and colleges
- Department for Education cyber security standards for schools and colleges
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes
- LGfL SafeguardED online-safety, filtering and monitoring, and generative AI resources
- National Cyber Security Centre guidance
- Ofcom online-safety information and reporting routes

Appendix – Roles

All staff

- Read and follow Part One of KCSIE 2026 and the College safeguarding and online-safety policies. Staff working directly with children and leaders must also read the additional KCSIE information required for their role.
- Complete induction and regular safeguarding updates, including online safety and filtering and monitoring responsibilities.
- Model safe, professional and lawful use of technology.
- Maintain supervision, professional curiosity and boundaries.
- Report concerns, filtering failures, overblocking, suspicious activity, loss of data and cyber incidents promptly.
- Do not investigate safeguarding concerns independently or view or forward illegal imagery.
- Use authorised systems and protect credentials and information.
- Provide accessible, age-appropriate online-safety education relevant to role.

Principal

- Foster a safeguarding culture in which online safety is fully integrated.
- Ensure the DSL, Executive Lead for filtering and monitoring, IT staff and DPO have authority, training, time and resources.
- Ensure annual online-safety and filtering and monitoring reviews are completed, documented and reported.
- Ensure significant risks are escalated and actions completed.
- Ensure staff and governors receive appropriate training and updates.
- Take overall executive responsibility for information security, data management and serious incident arrangements.

Designated Safeguarding Lead / Online Safety Lead

- Take lead responsibility for safeguarding and child protection, including online safety and understanding filtering and monitoring systems and processes.

- Work with Graeme Lavery, Vice Principal Finance and Resources and Executive Lead for filtering and monitoring, and IT support on reviews, checks, documentation and improvement.
- Ensure online incidents are assessed, recorded, referred and supported as safeguarding matters where appropriate.
- Maintain knowledge of emerging risks, local context and current guidance.
- Coordinate staff training and ensure reporting routes are understood.
- Review anonymised incident patterns, student voice and monitoring information.
- Ensure non-attendance, exploitation, child-on-child abuse, mental health, radicalisation and other safeguarding themes are considered where online activity is relevant.
- Report assurance, risks and actions to senior leaders and governors.

Governing Body, led by Online Safety / Safeguarding Link Governor

- Approve the policy and review its effectiveness.
- Ensure appropriate filtering and monitoring systems are in place and their effectiveness is reviewed at least annually.
- Undertake safeguarding and online-safety training sufficient to provide strategic challenge.
- Receive assurance on risks, incidents, curriculum, staff training, technical controls and actions.
- Challenge overreliance on technical controls and ensure student welfare, accessibility and educational access are balanced.
- Ensure serious or persistent gaps are addressed and resourced.

Personal Development Lead

- Coordinate a planned and responsive online-safety curriculum within personal development.
- Use safeguarding intelligence and student voice to adapt content.
- Ensure coverage includes relationships, consent, media literacy, AI, cyber security, exploitation, scams, radicalisation and reporting.
- Evaluate participation, understanding and areas requiring reinforcement.

Curriculum Area Managers and Tutors

- Embed relevant online safety within curriculum and tutorial activity.
- Ensure teaching technologies and AI services are approved and suitable.
- Risk assess sensitive content and maintain appropriate supervision.
- Respond promptly to disclosures, harmful behaviour and technical concerns.
- Promote academic integrity, critical evaluation and respectful online participation.

IT Systems and Infrastructure Manager

- Operate and maintain approved filtering, monitoring, security, identity and logging systems.
- Support documented checks and the annual effectiveness review.
- Provide the DSL and senior lead with intelligible information on scope, settings, limitations, incidents and changes.
- Maintain controlled access to monitoring data and ensure technical staff understand safeguarding escalation.
- Record material changes, tests, outages, exceptions and remedial actions.
- Escalate safeguarding and cyber concerns promptly and preserve evidence lawfully.
- Verify annually that descriptions of technical systems in this policy remain accurate.

Data Protection Officer (DPO)

- Advise on compliance with data protection laws, privacy, monitoring, AI, information sharing and impact assessments.
- Support proportionate safeguarding information sharing and ensure data protection is not misapplied as a barrier to protecting a child or adult at risk.
- Advise on breaches, retention, access, processor arrangements and rights.
- Work with safeguarding and IT colleagues where data and cyber incidents create welfare risk.

Volunteers and contractors, including tutors

- Follow College safeguarding, conduct, confidentiality and acceptable-use requirements.

- Use only authorised accounts, devices and communication routes.
- Report concerns immediately to the nominated College contact or safeguarding team.
- Do not contact students through personal accounts or retain student information outside authorised systems.

Students

- Use technology safely, respectfully, lawfully and for authorised purposes.
- Protect passwords and accounts and report loss, compromise or suspicious messages.
- Do not bully, harass, threaten, exploit, impersonate or create or share harmful content.
- Do not create, request, alter or share nudes, semi-nudes, deepfakes or deep nudes.
- Do not bypass College controls or interfere with systems.
- Seek help early and report concerns involving themselves or others.
- Follow staff direction regarding devices, recording, assessment and AI use.

Parents/carers

- Support safe and responsible technology use and discuss online experiences openly.
- Report concerns to the College rather than escalating conflict through social media.
- Work with the College on safeguarding and support plans.
- Respect privacy and consent when photographing, recording or posting College-related activity.
- Keep emergency and contact information current.

External groups

- Comply with safeguarding and online-safety conditions for use of College premises, networks, devices or students' data.
- Provide suitable supervision and obtain approval before using technology with students.
- Report incidents and cooperate with College safeguarding and technical enquiries.
- Ensure any independent filtering, monitoring, communication or recording arrangements are compatible with College expectations.

Version	Date	Summary of change	Approval
2026–27	6 September 2026	Updated from the 2025–26 policy while retaining the original style and local accountability model. Strengthened for KCSIE 2026, including the annual filtering and monitoring effectiveness review, AI-generated and digitally manipulated imagery, synthetic media, wearable technology, data protection changes and a comprehensive single-document approach.	Executive 09/09/2026
2025–26	September 2025	Previous approved policy.	Superseded on approval of this version