ASHVILLE

Online Safety Policy

Member of staff responsible:

Senior IT Operations Manager and the Designated Safeguarding lead (DSL)

Last reviewed: November 2026

Next review due: November 2027

The policy requires Governor approval

Location: Office 365/Every/Website

Definition of Terms

AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CEOP	Child Exploitation and Online Protection Centre
College	Ashville College, including Ashville Acorns Pre-Prep (including Reception), Prep School, Senior School and Sixth Form
Cyberbullying	Bullying that takes place over digital devices like cell phones, computers, and tablets
College Network	Any IT system or service that is owned or managed by the College. This includes but is not limited to things such as Microsoft365, PASS, ISAMS, SOCS, Evolve
DPA	Data Protection Act 2018 and the General Regulations on Data Protection
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessments
DSL	Designated Safeguarding Lead
EYFS	Early Years Foundation Stage
FOI	Freedom of Information
Watchguard / Securly	Software designed to filter internet access across the College
UK GDPR	UK General Data Protection Regulation
Governors	Directors of Ashville College Trustee Limited
Head	Head of the College
ICO	Information Commissioners Office - UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
ICT	Information and Communications Technology
INSET	In Service Training Day

LADO (LOCAL AUTHORITY DESIGNATED OFFICER)	Local Authority Designated Officer
PC	Personal Computer
PCI	Payment Card Industry
Pupils	Pupils who attend the College including pupils in the Early Years Foundation Stage (EYFS)
PSHE	Personal, Social and Health Education
SMT	Senior Management Team (Senior School)
Staff	Any member of the staff employed by the College in either a teaching or non-teaching role, members of the Governing Body and Volunteers working within the College
USB	An interface that enables communication between devices i.e. a computer and a flash drive, digital camera, keyboards and printers

Policies to be read in conjunction with this policy

- Acceptable Use Policy – **Pupils and Staff**
- Anti-bullying Policy
- Child Protection Policy
- College Behaviour Policy
- Data Protection Policy
- Relationships and Sex Education Policy
- Searching Pupils and their Possessions Policy
- Whistleblowing Policy

Other documents to be read in conjunction with this policy

- Images of Pupils – Taking, Storing and Using
- Procedure on Removal from the College
- Staff Code of Conduct

The following guidance should also be referred to when relevant

- Keeping Children Safe in Education (September **2026)**
- North Yorkshire Safeguarding Children Partnership
- Teaching Online Safety in Schools

Policy Development and Review

The Online Safety Policy has been developed by the Online Safety Committee, made up of:

- Senior leaders

- Designated safeguarding lead (DSL)
- Online Safety Lead
- Staff – including teachers/support staff/technical staff
- Governors

Schedule for development, monitoring and review

The Online Safety Policy was approved by the school governing body on:	
The implementation of the Online Safety Policy will be monitored by:	The Senior ICT Manager Designated Safeguarding Lead Online Safety Committee
Monitoring will take place at regular intervals:	Annually
The governing body will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Committee (which will include anonymous details of online safety incidents) at regular intervals:	As required on a termly basis
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external agencies will be informed, as appropriate:	Local Authority safeguarding officer, Police

Process for monitoring the impact of the Online Safety Policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring date for network activity
- Surveys/questionnaires of:
    - pupils
    - staff
    - parents and carers

Statutory Guidance and Department for Education Standards:

The following legislation and statutory guidance underpin the College's approach to online safety, safeguarding, data protection and the responsible use of technology.

- Keeping Children Safe in Education 2026 – Department for Education statutory guidance
- DfE Filtering and Monitoring Standards for Schools and Colleges (updated September 2026)
- Education Act 2002 – Legislation
- Education and Inspections Act 2006 – Legislation
- UK General Data Protection Regulation (UK GDPR) – ICO guidance

- Data Protection Act 2018 – Legislation
- Human Rights Act 1998 – Legislation
- Counter-Terrorism and Security Act 2015 (Prevent Duty) – Legislation
- The Prevent Duty: Practical Guidance for Designated Safeguarding Leads (DfE, updated October 2026)
- Voyeurism (Offences) Act 2019 – Legislation
- Online Safety Act 2023 – Legislation
- Protection of Children Act 1978 – Legislation
- Coroners and Justice Act 2009 – Legislation
- Sexual Offences Act 2003 – Legislation
- Malicious Communications Act 1988 – Legislation
- Communications Act 2003 – Legislation

Introduction

The College is a caring community rooted in Methodist values, where the safety and wellbeing of all pupils and staff are a priority.

Digital technology plays an important role in teaching, learning and communication, providing valuable opportunities for education and personal development. The College recognises the benefits of technology alongside the potential risks and is committed to helping pupils develop the knowledge, skills and confidence to use it safely and responsibly.

Keeping Children Safe in Education (KCSIE) 2026 identifies four broad areas of online safety risk, commonly known as the **4 Cs**:

- **Content:** Exposure to illegal, inappropriate or harmful material, including pornography, discrimination, misogyny, self-harm, suicide, extremism, misinformation and violent content.
- **Contact:** Harmful interactions with others online, including grooming, exploitation, peer pressure and risks associated with artificial intelligence (AI) applications that simulate human interaction.
- **Conduct:** Online behaviour that causes or increases the risk of harm, including cyberbullying, sharing nudes or semi-nudes, harassment and the creation or sharing of AI-generated explicit images or deepfakes.
- **Commerce:** Risks associated with online gambling, inappropriate advertising, phishing, scams and financial exploitation.

The College adopts a whole-school approach to online safety, combining education, appropriate filtering and monitoring, clear reporting procedures and safeguarding support. Through the curriculum, including PSHE and computing, pupils are taught to recognise online risks, evaluate digital information critically, protect their personal information and seek help when needed.

The College recognises that online risks cannot be eliminated entirely. Our approach focuses on prevention, early identification and proportionate responses, while developing pupils' digital literacy, resilience and independence. Online safety is a shared responsibility, and this policy should be read alongside the College's Child Protection, Behaviour, Anti-Bullying, Acceptable Use, Staff Code of Conduct and Data Protection policies.

The College is committed to protecting personal information and respecting individuals' privacy in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Pupils and staff are expected to use technology responsibly, including taking appropriate precautions when sharing information online.

1 Child Protection

1.1 The College recognises that internet safety is a child protection and general safeguarding issue. The DSL Deputy DSLs and the Senior IT Operations Manager have been trained in safety issues involved with the misuse of the internet and other mobile electronic devices. They work to promote a culture of responsible use of technology that is consistent with the ethos of the College. All of the staff, especially those with pastoral responsibilities, receive training in online safety issues.

1.2 Ashville College has a programme of online safety which ensures that all year groups in the College are educated, in an age-appropriate way, in the risks and reasons why they need to behave responsibly online. The Head of EYFS, Head of Prep and Head of Senior School are responsible for overseeing the programme across the College.

2 Scope of the Policy

2.1 This policy applies to all staff, pupils, parents/carers, visitors and community users who have access to and are users of College ICT systems and services, both in and out of the College.

2.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published College Behaviour Policy.

2.3 The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of College.

3 Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the College:

3.1 **Governors**

Governors are responsible for the approval of the Online Safety Policy, and for reviewing the effectiveness of the policy ensuring it is disseminated to the wider College community. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

The role of the Governing Body does include ensuring that the statutory requirements of Keeping Children Safe in Education September **2026** are complied with. In relation to online safety this includes:

The Governing Body will ensure that:

- online safety remains a running and interrelated theme within the College's safeguarding arrangements, curriculum, staff training, policies and procedures;
- appropriate filtering and monitoring systems are in place on College devices and networks;
- a member of the Senior Leadership Team is identified as the strategic lead responsible for filtering and monitoring;
- the effectiveness of the College's filtering and monitoring provision is formally reviewed at least once every academic year;
- the review is led by the responsible Senior Leadership Team member, with support from the Designated Safeguarding Lead and IT staff;
- the findings of filtering and monitoring reviews, identified weaknesses and required actions are reported to the Governing Body;
- the College's approach is informed by the Department for Education's filtering and monitoring standards, the Prevent Duty risk assessment and the risks faced by the College's pupils;
- harmful and inappropriate content is blocked without unreasonably restricting teaching, learning or access to appropriate safeguarding information;
- effective monitoring arrangements are in place that meet the College's safeguarding needs, including risks presented by generative artificial intelligence; and
- relevant staff understand the systems in place, their responsibilities and the procedure for reporting and escalating concerns.

The role of the Safeguarding Governor includes:

3.1.1 regular meetings with the Online Safety Lead and the DSL
3.1.2 attendance at Safeguarding committee meetings (by one of the Safeguarding Governors)
3.1.3 regular monitoring of online safety incident logs and responding appropriately to identified needs
3.1.4 reporting to Full Governor's Committee each term.

3.2 The Head

The Head and member of SLT responsible for Filtering & Monitoring should ensure:

3.2.1 the Governors comply with the online safety aspects of Keeping Children Safe in Education (**September 2026**) documentation;
3.2.2 the safety (including online safety) of all members of the College community;
3.2.3 effective and regular training about online safety is provided for the whole College community and a log is kept of the staff who complete the training;
3.2.4 Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education, health and safety or child protection;
3.2.5 effective communication with parents/carers about safe practices when using online technology's and support them in talking to their children about these issues;
3.2.6 effective filtering, monitoring and security systems are set up;
3.2.7 Annual Filtering and Monitoring testing is carried out and reported upon
3.2.8 there are effective procedures in place in the event of an online safety allegation which are known and understood by all members of staff;

3.2.9 establishing and reviewing the College online safety policy and documents and making them available on the College website;
3.2.10 the College's DSL should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.
3.2.11 That the staff involved in online safety systems and procedures for the College have sufficient capacity to manage them.

3.3 The Senior Leadership Team

The Senior Leadership Team should:

3.3.1 liaising with staff, ICT Technical staff, Online Safety Governor, ELT and partner agencies on all issues related to online safety;
3.3.2 ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
3.3.3 providing training and advice for staff and keeping a log of staff who complete training about online issues;
3.3.4 keep a log of staff, pupils and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology;
3.3.5 receive and respond to reports of online safety incidents and create a log of incidents and outcomes to inform future online safety developments;
3.3.6 Coordinating and reviewing online safety education programme in the College (or working in partnership with the Personal, Social, Health, Education (PSHE) and/or Computing lead).
3.3.7 Oversee and monitor the Smart-Device-Free environment and policy for Prep and Senior School.

3.4 Online Safety Lead (Senior IT Operations Manager)

The Online Safety Lead;

3.4.1 leads the Online Safety Committee;
3.4.2 takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the College online safety policy/documents;
3.4.3 ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
3.4.4 provides/organises training and advice for staff on online safety matters;
3.4.5 liaises with the College ICT technical staff;
3.4.6 receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
3.4.7 meets termly with the Safeguarding Governor to discuss current issues and review incident logs and filtering;
3.4.8 reports regularly to the ELT;
3.4.9 attends the relevant committee of the Governing Body.
3.4.10 Annually tests the filtering and monitoring effectiveness and reports to governors.
3.4.11 The Designated Safeguarding Lead retains overall responsibility for safeguarding and online safety. The Online Safety Lead provides operational and technical support.

3.5 Senior IT Operations Manager and Technical Staff

The Senior IT Operations Manager and Technical Staff are responsible for ensuring;

3.5.1 that the College's technical infrastructure is secure and is not open to misuse or malicious attack and meets requirements for filtering and monitoring and any other relevant cyber security legislation;

3.5.2 that the College meets required online safety technical requirements including any requirements of 'Keeping Children Safe in Education' (September **2026)**, PCI Compliance and the UK GDPR that may apply;

3.5.3 that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are-changed in line with current best practice guidance;

3.5.4 that they keep up to date with online safety technical information ~~and,~~ cyber security and data protection best practice in order to effectively carry out their online safety role and to inform and update others as relevant;

3.5.5 Maintain a cyber security risk assessment

3.5.6 that the use of the network/internet/ remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead/ Head of Senior School/ Head of Lower School/Head of Upper School/Head of Sixth Form/ Head of Prep/ Deputy Head of Prep School for investigation/ action/sanction;

3.5.7 that monitoring software/systems are implemented and updated as agreed in College policies.

3.5.8 That reporting system meets the requirements of Keeping Children Safe in Education (September **2026**).

3.6 **All Staff**

In addition to understanding the elements covered in the Staff Acceptable Use Policy (AUP), all staff are responsible for ensuring that;

3.6.1 they have an up-to-date awareness of online safety matters and of the current College Online Safety Policy and practices;

3.6.2 they attend the training provided by the College about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the College online safety policy, Acceptable Usage and Child Protection Policies;

3.6.3 they have read, understood and signed the College Staff Acceptable Usage Policy AUP;

3.6.4 they do not 'be-friend' any pupil or pupil family member on social media in a social context whilst the pupils are at the College or for five years after they have left;

3.6.5 online safety issues are embedded in all aspects of the curriculum and other College activities;

3.6.6 pupils understand and follow the College's Online Safety and acceptable usage policies;

3.6.7 pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

3.6.8 they monitor ICT activity in lessons, extracurricular and extended College activities;

3.6.9 in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;

3.6.10 all staff should be aware that emails can be part of Freedom of Information and subject access requests so all correspondence needs to be professional, courteous and respectful;

3.6.11 if confidential information/information under the data protection act is being sent by email it must be sent through the secure email system, e.g. the Egress system.

3.6.12 Data protection procedures and policies must not prevent the sharing of safeguarding information if it were to jeopardise an investigation or response to an incident.

3.7 Designated Safeguarding Lead

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from;

3.7.1 sharing of personal data;
3.7.2 access to illegal/inappropriate materials;
3.7.3 inappropriate online contact with adults/strangers;
3.7.4 potential or actual incidents of grooming;
3.7.5 cyber-bullying.
3.7.6 the 4 Cs, conduct, contact, content and commerce
3.7.7 The Designated Safeguarding Lead retains overall responsibility for safeguarding and online safety. The Online Safety Lead provides operational and technical support.

3.8 Online Safety Committee

The **Online Safety Committee** provides a consultative group that has wide representation from the College community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the **Online Safety Committee** will assist the Online Safety Lead (or another relevant person) with;

3.8.1 the production/review/monitoring of the College Online Safety Policy/ documents;
3.8.2 mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression;
3.8.3 monitoring network/internet/incident logs related to safeguarding issues;
3.8.4 consulting stakeholders – including parents/carers and the pupils about the online safety provision
3.8.5 Review and monitor the use of AI across the college.

3.9 Pupils

Pupils:

3.9.1 are responsible for using the College ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to 'agree to' before being given access to College systems;
3.9.2 have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, including safe and responsible use of AI
3.9.3 need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
3.9.4 will be expected to know and understand policies on the use of mobile devices and other smart devices. They should also know and understand policies on the taking/use of images and on cyber-bullying;

3.9.5 should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

3.10 **Pupils – EYFS Setting**

EYFS has a duty to provide children with quality internet access as part of their learning.

3.10.1 Internet access is tailored expressly for educational use and includes appropriate filtering.
3.10.2 Pupils in EYFS learn appropriate internet use.
3.10.3 Staff guide pupils in online activities that will support their learning journeys.
3.10.4 Staff are responsible for ensuring that material accessed by the children is appropriate.
3.10.5 Children do not access the internet unattended.
3.10.6 Internet safety in EYFS depends on staff, parents, carers and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones.
3.10.7 Filters are in place to limit internet access and to monitor effectiveness.
3.10.8 Permission from parents or carers for featuring their child on the website is requested when each child starts College and parents/carers wishes are followed at all times.
3.10.9 Online learning journals are secure, and parents can only access their own child's journal.

3.11 **Parents/Guardians**

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile and smart devices in an appropriate way. Parents are also responsible for monitoring their children's internet use and for ensuring that their children are not involved in any incidents of cyber-bullying.

It is recognised that not all parents and carers may feel equipped to protect their child(ren) when they use electronic equipment at home hence the College organises occasions and age-appropriate information evenings for parents/guardians when a specialist offers advice about the potential hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their child(ren) without curbing their natural enthusiasm.

The College seeks to work closely with parents and guardians in promoting a culture of online safety. The College will always contact parents/guardians if there are any worries about a child or young person's behaviour in this area, and parents/guardians are encouraged to share any worries with us.

Parents and guardians will be encouraged to support the College in promoting good online safety practice and to follow guidelines on the appropriate use of;

3.11.1 digital and video images taken at College events;
3.11.2 access to parents' sections of the website on online pupil records;
3.11.3 their children's personal devices in the College.

Parents and guardians will be responsible for:

3.11.4 endorsing (by signature) the Pupil Acceptable Usage Policy within the Prep School;

3.11.5 Endorsing that they do not use social media to criticise or make inappropriate comments about the College or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/guardian, they have any concerns about anything which happens in the College then please contact the College directly.

4 Policy Statements

4.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the College's online safety provision. Children and young people need the help and support of the College to recognise and avoid online safety risks and build their resilience.

The College will provide age-appropriate and developmentally appropriate education about online safety throughout the curriculum.

Teaching will be adapted where necessary for pupils with special educational needs and/or disabilities and other vulnerabilities.

The curriculum will include:

- the four Cs of online risk: content, contact, conduct and commerce;
- misinformation, disinformation, fake news and conspiracy theories;
- healthy and respectful online relationships;
- consent, pressure, coercion and the sharing of images;
- making and sharing nudes and semi-nudes;
- AI-generated and AI-manipulated intimate images;
- deepfakes and nudification tools;
- how generative AI applications may simulate human interaction;
- grooming, exploitation and harmful contact;
- pornography, misogyny and harmful online influencers;
- online bullying, sexual harassment and harmful sexual behaviour;
- privacy, personal information and digital footprints;
- how to recognise synthetic or manipulated content;
- the safe, ethical and responsible use of generative AI;
- how filtering and monitoring help to keep pupils safe; and
- how and where pupils can report concerns and obtain support.

Pupils will be taught that creating or sharing a fake, manipulated or AI-generated intimate image can cause real harm and will be treated seriously, even when no genuine nude image existed. Teaching will emphasise that pupils who experience harm will be supported and should report concerns without fear of blame or shame.

4.2 **Education – Parents/Guardians**

The College will provide parents and carers with appropriate information about emerging online risks and the measures used to safeguard pupils. This will include information about:

- the College's filtering and monitoring arrangements;
- deepfakes, nudification tools and AI-generated intimate images;
- making and sharing nudes and semi-nudes;
- age restrictions and privacy settings;
- signs that a child may be experiencing online harm;
- how parents and carers can report concerns to the College; and
- sources of support, reporting and image-removal services.

Parents and carers will be encouraged to speak with the College promptly if they become aware of an online-safety concern. The College will respond in a supportive, child-centred and proportionate manner.

4.3 **Education and Training – Staff**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

4.3.1 A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.

4.3.2 It is expected that some staff will identify online safety as a training need within their personal appraisal process:

4.3.3 All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the College Online Safety Policy and Acceptable Use Agreements:

4.3.4 The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations:

4.3.5 This Online Safety Policy and its updates will be presented to and discussed by staff in staff/INSET days:

4.3.6 The Online Safety Lead will provide advice/guidance/training to individuals as required.

4.4 **Training – Governors**

Governors will be offered online safety training through participation in College training/information sessions for staff or parents.

5 ICT Acceptable Use Policy

Online safety is a whole College responsibility, and all staff and pupils are required to adhere to an ICT Acceptable Use Policy, which incorporates the following guidelines in age-appropriate ways:

5.1 **Treating others with Respect**

5.1.1 The College expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the College's Code of Conduct for Pupils, Prep School Rules, Senior School and Sixth form rules which are

discussed with pupils in the Prep School and Senior School and copies of which are displayed in the schools.

5.1.2 The College expects a degree of formality in communications between staff and pupils and would not in normal circumstances expect them to communicate with each other by text or mobile phone.

5.1.3 Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The College is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation, disability or Special Educational Needs.

6 Filtering and Monitoring

The College will maintain appropriate filtering and monitoring systems on College networks and College-owned devices. These systems form an important part of the College's wider safeguarding arrangements but do not replace effective supervision, education, professional curiosity or appropriate staff response.

A member of the Senior Leadership Team will be identified as the strategic lead responsible for filtering and monitoring. The strategic lead will work with the Designated Safeguarding Lead, Senior IT Operations Manager, relevant technical staff and external service providers.

The Designated Safeguarding Lead will take lead responsibility for safeguarding and online safety. IT staff will have technical responsibility for maintaining, testing and supporting the systems. Decisions about safeguarding thresholds, the welfare of a child and the response to safeguarding alerts remain the responsibility of the Designated Safeguarding Lead or a deputy.

The effectiveness of the College's filtering and monitoring provision will be formally reviewed at least once every academic year and additionally when:

- there is a significant safeguarding incident;
- a new or emerging online risk is identified;
- significant changes are made to the College's network, devices, software or service providers;
- a new pupil-facing technology or generative AI service is introduced; or
- testing or monitoring identifies a possible weakness.

The review will include recorded checks that filtering is working appropriately on all internet-connected devices and in all relevant locations. This will include, where applicable, EYFS, Prep, Senior School, Sixth Form, boarding provision, remote-access arrangements, College-owned mobile devices and personal devices permitted to connect to College networks.

The review will consider:

- the age range and developmental needs of pupils;
- pupils with special educational needs and/or disabilities;
- pupils who may be at increased risk of harm or exploitation;
- access outside the normal College day;
- how frequently and in what circumstances pupils access the College's IT systems;
- emerging online risks and changes in technology;
- the effectiveness and timeliness of monitoring alerts;
- whether alerts reach appropriately trained staff;
- arrangements for responding to alerts outside normal College hours;

- the effectiveness of escalation and recording procedures;
- the use of generative AI and AI-enabled services;
- whether harmful and inappropriate content is blocked appropriately; and
- whether filtering causes unreasonable restrictions on teaching, learning or access to safeguarding information.

A written record will be kept of all formal reviews and checks. This will include the date, scope and outcome of testing, any identified weaknesses, required actions, the person responsible for each action and the date on which the action was completed.

Filtering and monitoring alerts that indicate a possible safeguarding concern must be shared promptly with the Designated Safeguarding Lead or a deputy and recorded on the College's safeguarding recording system. Technical incidents that do not present a safeguarding concern may be recorded within the incident log. Where there is uncertainty, the matter must be treated as a potential safeguarding concern and referred to the Designated Safeguarding Lead.

Requests to unblock websites or online services must be authorised, time-limited, based on a clear educational need and recorded. The potential safeguarding, Prevent Duty, data-protection and security implications must be considered before access is permitted. Filtering and Monitoring arrangements support the College's Prevent Duty obligations and are informed by the prevent risk assessment.

The College will communicate appropriately with parents and carers about the filtering and monitoring systems used to safeguard pupils while they use College devices and networks.

All safeguarding concerns are written in CPOMS and there is Filtering & Monitoring log that keeps a record any filtering monitoring alert and actions taken.

7 Generative Artificial Intelligence

The College recognises that generative artificial intelligence can support teaching, learning and College administration. It can also create safeguarding, ethical, information-security, data-protection, accuracy, bias, copyright and intellectual-property risks.

Generative AI includes technology that can create or manipulate text, images, audio, video or other content and applications that simulate interaction with another person. Risks may include:

- exposure to harmful, inaccurate, biased or age-inappropriate content;
- AI applications simulating friendships or relationships with children;
- grooming, coercion, exploitation or sexualised interaction;
- the creation or manipulation of nude, semi-nude or sexually explicit images;
- sexually explicit deepfakes and the use of nudification tools;
- impersonation, bullying, harassment, fraud or reputational harm;
- the disclosure or processing of personal, confidential or safeguarding information;
- misinformation and convincing synthetic content;
- attempts to bypass filtering, monitoring or other safeguarding controls; and
- reliance on inaccurate AI-generated information or advice.

Only generative AI tools approved by the College may be used for College purposes. Approval will take account of the service's age restrictions, terms of use, privacy arrangements, use and retention of data, moderation, safety controls, security and suitability for the intended users.

Before a pupil-facing generative AI service is introduced, the College will complete an appropriate assessment of its safeguarding, data-protection and information-security risks. A data protection impact assessment will be completed where required.

Filtering and monitoring requirements apply to generative AI services, including stand-alone applications and AI functions embedded within search engines, learning platforms, productivity software, messaging services and other online tools.

Staff and pupils must not enter personal data, special-category data, confidential College information or safeguarding information into a generative AI system unless the specific system and proposed use have been formally approved.

Staff remain professionally responsible for any material produced or informed by AI. AI must not be relied upon to make decisions about safeguarding, child protection, behaviour, discipline, admissions, assessment or an individual pupil's welfare.

Pupils must not use AI to create, request, alter, distribute or threaten to distribute harmful, abusive, discriminatory, sexual or intimate content. This includes fake or manipulated content that appears to depict a real person, regardless of whether the image, video or audio is wholly synthetic.

Any safeguarding concern involving AI must be reported immediately to the Designated Safeguarding Lead or a deputy and managed in accordance with the Child Protection Policy. Technical concerns must also be reported to the Senior IT Operations Manager.

8 Deepfakes, Nudes and Semi-nudes

For the purposes of this policy, "making or sharing nudes and semi-nudes" means the creation, sending or posting of nude or semi-nude visual content involving a person under the age of 18. Visual content includes photographs, videos, livestreams and images that have been created, altered or manipulated using artificial intelligence.

This includes:

- images or videos taken by a child of themselves or another child;
- consensual or non-consensual sharing;
- images obtained through pressure, coercion, grooming or exploitation;
- images shared beyond the intended recipient;
- sexually explicit deepfakes;
- images altered to make a person appear nude or sexualised;
- content created through nudification tools; and
- wholly synthetic content that appears to depict a real child.

The College recognises that an AI-generated or manipulated image can cause significant and lasting harm even where the child did not create, pose for or share an original nude image.

Taking and sharing nude images of a person under 18, including images generated or manipulated using AI, may constitute a criminal offence. The College will, however, respond in a child-centred and proportionate manner. Staff will explain in an age-appropriate and reassuring way that the law exists to protect children and young people and not to unnecessarily criminalise them.

All incidents must be reported immediately to the Designated Safeguarding Lead or a deputy. The Designated Safeguarding Lead will lead the response in accordance with the Child Protection Policy and current UKCIS guidance on sharing nudes and semi-nudes.

The response will consider each incident individually, including:

- the ages and developmental stages of the children;
- any age difference or imbalance of power;
- whether the content was created or shared consensually;
- whether pressure, coercion, threats, grooming or exploitation were involved;
- whether the content has been shared more widely;
- whether an adult is involved;
- whether the incident forms part of a pattern of behaviour;
- the vulnerability and needs of the children involved;
- the risk of bullying, harassment, retaliation or further distribution;
- whether immediate action is required to secure a device or preserve evidence; and
- whether children's social care, the police or another external agency should be involved.

Consensual image-sharing between children of a similar age may require a different response from non-consensual, coercive or exploitative behaviour. It must nevertheless be treated as a safeguarding matter, and children must be supported to understand the risks and the law.

Children affected by an incident will be listened to, reassured, supported and protected from blame or shame. The College will consider appropriate support for the child depicted, the child who created or shared the content and any other affected pupils.

The College will take proportionate action to reduce the risk of continued sharing and will provide information about relevant reporting and removal services, including Childline and the Internet Watch Foundation's Report Remove service.

9 Cyberbullying

Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The College's Anti-bullying Policy sets out preventative measures and the procedures that will be followed where cases of bullying are discovered.
Proper supervision of pupils plays an important part in creating a safe ICT environment at College; but everyone needs to learn how to stay safe out of College.
Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and they should not be afraid to report the matter.

10 Keeping the College's Network Safe

10.1 Certain sites are blocked by the College's filtering system, and the system monitors all use of the network, and the Senior IT Operations Manager will oversee the checking of this on a regular basis.

10.2 The system also monitors e-mail traffic and blocks SPAM and certain attachments.

10.3 All pupils from Year 3 upwards are issued with their own personal College e-mail address. Access is via a personal LOGIN, which is password protected. Guidance is given on the reasons for always logging off and for keeping all passwords secure.

10.4 There is strong anti-malware protection on the College network, which has been installed by IT Support.

10.5 Passwords **are an Important Element of Keeping the Users of the College ICT System Safe**

10.5.1 Use of Passwords for Staff and Governors

10.5.1.1 Passwords or encryption keys should not be recorded on paper or in an unprotected file.
10.5.1.2 Passwords should be changed at least every 61 days.
10.5.1.3 Users should not use the same password on multiple systems or attempt to 'synchronise' passwords across systems.

10.5.2 Use of Passwords for Pupils

10.5.2.1 Pupils should only let College staff know their in-school passwords.
10.5.2.2 Pupils should not share their password with another pupil/sibling.
10.5.2.3 Pupils should inform staff immediately if passwords are traced or forgotten.

Acceptable Use Policies for ICT usage are given to staff and pupils. Copies of this are displayed in classrooms around the College. The College will impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices (see Appendix 4 and Appendix 5).

11 Technical – Infrastructure/Equipment, Filtering/Monitoring and Reporting

11.1 The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

11.1.1 College technical systems will be managed in ways that ensure that the College meets recommended technical requirements:
11.1.2 There will be regular reviews and audits of the safety and security of College technical systems:
11.1.3 Servers, wireless systems and cabling are securely located, and physical access is restricted:
11.1.4 All users will have clearly defined access rights to College ICT systems:
11.1.5 All users will be identifiable to filtering and monitoring systems
11.1.6 All users will be provided with a username and secure password by the Senior IT Operations Manager who will keep an up-to-date record of users and their usernames. Users will be required to change their password every 60 days:
11.1.7 The 'administrator' passwords and private encryption keys for the College system, used by the Senior IT Operations Manager (or other person) must also be available to the Head or other nominated senior leader and kept in a secure place (e.g. College safe):
11.1.8 Users are responsible for the security of their username and password, must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there is a breach of security:
11.1.9 The Senior IT Operations Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations:
11.1.10 Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered through 'Fortigate'. Content lists are regularly updated, and internet use is logged and regularly monitored:

11.1.11 The Internet filtering should also ensure that children are safe from terrorist and extremist material when accessing the internet:

11.1.12 The internet filtering will be age appropriate and also consider the needs of individual roles within the College. The College will seek to ensure 'over-blocking' is kept to a minimum.

11.1.13 The College provides enhanced user-level filtering through the use of 'a Fortigate Web Filter'. In the event that the Senior IT Operations Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head (or other nominated senior leader, excluding the Senior IT Operations Manager):

11.1.14 Requests from staff for sites to be removed from the filtered list will be considered by the Senior IT Operations Manager and the relevant Deputy Head. If the request is agreed, this action will be recorded:

11.1.15 Reports on internet usage, safeguarding risk and other trends will be regularly delivered to the appropriate staff.

11.1.16 College IT Support staff passively monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy:

11.1.17 Remote management tools are used by staff to control workstations and view user's activity:

11.1.18 An appropriate system is in place for users to report any actual/potential technical incident/online safety incident to the Senior IT Operations Manager see Appendix 3:

11.1.19 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up-to-date EDR software:

11.1.20 An agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the College system:

11.1.21 An agreed policy is in place regarding the extent of personal use that users (staff/pupils) are allowed on College devices that may be used out of College:

11.1.22 An agreed policy is in place that forbids staff from installing programmes on College workstations/portable devices:

11.1.23 An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on College workstations/portable devices:

11.1.24 Personal data cannot be sent over the internet to non-College systems or taken off the College site unless agreed by the Data Protection Officer. (Veritau is our contracted DPO).

12 Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

12.1 In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

12.2 Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites that the pupils visit. Searches should be logged on the Colleges web filter and checked for their appropriateness and if they pose a safeguarding risk.

12.3 It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Senior IT Operations Manager can temporarily remove these sites from the filtered list for the period of study. Any request to do so, should be recorded with clear reasons for the need.

12.4 Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information.

12.5 Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

13 Bring Your Own Device (BYOD) (Sixth Form Only)

13.1 Pupils in the sixth form bring their own laptops to use in College. Use of BYOD should not introduce vulnerabilities into existing secure environments and users should refer to the Acceptable Use Policy as well as Parental Information on Mobile Devices, but the following provide a brief overview of the key points:

13.1.1 The College has a set of clear expectations and responsibilities for all users:
13.1.2 The College adheres to the Data Protection Act principles:
13.1.3 All users are provided with and accept the Acceptable Use Policy:
13.1.4 All network systems are secure and access for users is differentiated:
13.1.5 Monitoring of websites and blocked websites occurs for any devices connected to the College's network
13.1.6 All users will use their username and password and keep this safe:
13.1.7 Pupils receive training and guidance on the use of personal devices:
13.1.8 Regular audits and monitoring of usage will take place to ensure compliance:
13.1.9 Any device loss, theft, **and** change of ownership of the device will be reported.

13.2 Social Media and Telephone Communication

13.3 The College Senior IT Operations Manager and IT Support staff have a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the College system and data and for training our teaching and support staff in the use of ICT. They monitor the use of the internet and e-mails and will report any observed inappropriate usage to the appropriate senior manager. It is the responsibility of all staff to report any inappropriate usage to the Senior IT Operations Manager. Access to sites of inappropriate content is blocked from the College network, as is access to social media sites.-Other exceptions include departments that have a legitimate need to engage on social media platforms. These users will receive appropriate training on the safe use of social media sites.

13.4 Appropriate Use of Email

13.4.1 Digital communications with pupils and parents/guardians should be on a professional level and only carried out using official College systems.
13.4.2 The College's email service should be accessed via the provided web-based interface by default.
13.4.3 Under no circumstances should staff or governors contact pupils, parents/guardians or conduct any College business using personal email addresses.
13.4.4 College email is not to be used for personal use.

13.4.5 All staff should be aware that emails can be part of Freedom of Information and subject access requests so all correspondence needs to be professional, courteous and respectful.

13.5 Appropriate use of Mobile Phones and smart devices

13.5.1 College mobile phones only should be used to contact parents/carers/pupils when on College business with pupils off site. Staff should not use personal mobile devices and under no circumstances should a pupil or parent/guardian be given a member of staff's personal mobile number.

13.5.2 Staff should not be using personal mobile phones unless sanctioned for work use or for Multi Factor Authentication purposes.

13.5.3 Visitors will be asked not to use their mobile phone whilst on site with any pupil presence due to all mobile phones containing a camera and to remove any smart devices or devices that can record.

13.5.4 Pupils should adhere to the rules and guidelines set out in the College Behaviour and acceptable use Policy regarding mobile phone and smart device use in College.

13.5.5 All pupils from years 7-11 will be required to put their phone and smart devices in a lockable YONDR pouch during form time in the morning.

13.5.6 All pupils will be able to unlock their pouches at the stations provided at the end of school.

13.6 Appropriate Use of Social Networking Sites

13.6.1 Staff should not access social networking sites on College equipment in school or at home that have not been pre-approved by the College.

13.6.2 Staff users and governors should not refer to any member of staff, the governing body, pupils, parents/carers, the College or any other member of the College community on any social networking site or blog in a derogatory way.

13.6.3 Pupils will not be allowed on social networking sites on College equipment that have not been pre-approved whether in College or at home. At home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

13.6.4 Pupils/Parents/guardians should be aware the College will investigate misuse of social networking if it impacts on the well-being of other pupils or members of the College community.

13.6.5 Parents/guardians and pupils will be informed that they do not use social media to criticise or make inappropriate comments about the College, an individual member of staff or another pupil as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/guardian, they have any concerns about anything which happens in College they should contact a member of staff.

13.6.6 If inappropriate comments are placed on social networking sites about the College or College staff then advice would be sought from the relevant agencies, including the police if necessary.

13.6.7 Pupils will be taught about online safety when using social networking sites.

14 Use of Digital and Video Images – Photographic, Video

14.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/guardians need to be aware of the risks associated with publishing digital images on the internet. Images online can be accessed by anyone and there is a risk that they could be used or altered by AI for harmful purposes. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The same issues can arise with digital recordings made of individuals.

14.2 The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

14.2.1 When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;

14.2.2 Written permission from parents or guardians will be obtained before photographs of pupils are published on the College website/social media/local press;

14.2.3 In accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their own children at College events for their own personal use (as such use as not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/guardians comment on any activities involving other pupils in the digital/video images;

14.2.4 Staff are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on, or processed thereafter, College equipment, the personal equipment of staff should not be used for such purposes;

14.2.5 Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute;

14.2.6 Pupils should not take, use, share, publish or distribute images (for example, video or photographs) of staff or pupils without their permission:

14.2.7 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

14.2.8 Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

14.2.9 A pupil's work can only be published with the permission of the pupil and parents or guardians.

14.2.10 The College will liaise with external providers and places visited on school trips to ensure they do not take photographs and use the images on their website/social media without permission of a member of staff from the College.

14.3 The Terms and Conditions that parents sign includes a section as follows:

You consent to us making use of information relating to your child (including photographs and video recordings), and (where appropriate) relating to you, whilst your child is at the College and after they have left for the purposes of:

- *managing relationships between the College and current pupils/parents and fulfilling our obligations under the contract with you;*
- *promoting the College to prospective pupils/parents;*
- *publicising the College's activities; and*
- *communicating with the College community and the body of former pupils.*

In respect of (ii), (iii) and (iv), this includes use of such information by the College in/on the College's prospectus (in whatever format or medium it is produced/made available), the College's website(s) and (where appropriate) the College's social media channels.

If you do not want your child's photograph or image to appear in any of the College's promotional material you must make sure your child knows this and must give notice to the Head, this notice will be acknowledged by the College.

14.4 Staff need to be mindful of the possible child protection issues associated with the possession of images of children and as such they are required to adhere to the following policy:

14.4.1 All images and video taken of individual pupils or groups of pupils must be uploaded **as soon as possible** to the College network;

14.4.2 All images and video of individual pupils or groups of pupils which are delivered to a member of staff as part of their professional work, for example, for an Art display or a marketing initiative, must **not** be stored on any personal computer, the hard drive of any College computer, the memory of any camera or similar device, any personal memory device or other transportable memory and should be uploaded immediately to the College network;

14.4.3 Any manipulation or images or video for any purpose including controlled assessment, coursework, marketing, etc., **must** be undertaken on the College network and the results of that manipulation stored on the network only. Exceptionally, Heads of Department may have occasion to transmit appropriate video and images to the awarding bodies and will be guided in that by the relevant regulations.

15 Data Protection

15.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act - 2018 which states that personal data must be;

15.1.1 fairly and lawfully processed;
15.1.2 processed for limited purposes;
15.1.3 adequate, relevant and not excessive;
15.1.4 accurate;
15.1.5 kept no longer than necessary;
15.1.6 processed in accordance with the data subject's rights;
15.1.7 secure;
15.1.8 only transferred to others with adequate protection and consent;

15.1.9 portable.

15.2 The College will ensure that;

15.2.1 it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
15.2.2 every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
15.2.3 all personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing';
15.2.4 it has a Data Protection policy;
15.2.5 it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
15.2.6 Veritau are appointed as the Data Protection Officer
15.2.7 risk assessments are carried out and risk management forms completed as required;
15.2.8 it has clear and understood arrangements for the security, storage and transfer of personal data;
15.2.9 data subjects have right of access and there are clear procedures for this to be obtained;
15.2.10 there are clear and understood policies and routines for the deletion and disposal of data;
15.2.11 there is a policy for reporting, logging, managing and recovering from information risk incidents;
15.2.12 there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
15.2.13 there are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner's Office;
15.2.14 appropriate data protection impact assessments have been conducted.

15.3 Staff must ensure that they;

15.3.1 at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
15.3.2 use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
15.3.3 transfer data using encryption and secure password protected devices.
15.3.4 Are aware of and adhere to the principles set out in Data protection Act 2018.

15.4 The storing of personal data on memory stick or any other removable media should be avoided. In exceptional circumstances, such as an immediate need in relation to a safeguarding incident, this may be necessary. If this is the case staff must ensure that;

15.4.1 They have consulted with a senior member of staff;
15.4.2 the data must be encrypted, and password protected;
15.4.3 the device must be password protected (many memory stick/cards and other mobile devices cannot be password protected;
15.4.4 the device must offer approved virus and malware checking software;
15.4.5 the data must be securely deleted from the device, in line with College policy once is has been transferred or its use is complete.

16 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the College currently considers the benefit of using these technologies for education outweighs their risks/disadvantages.

16.1 When using communication technologies, the College considers the following as good practice:

16.1.1 The official College e-mail service may be regarded as safe and secure and is monitored. Staff, Governors, volunteers and pupils should therefore use only the College email service to communicate with others when in College or on College systems i.e. by remote access).;

16.1.2 Users should be aware that e-mail communications may be monitored;

16.1.3 Users must immediately report, to the nominated person, in accordance with the College policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;

16.1.4 Any digital communication between staff, governors and pupils or parents/guardians (e-mail, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal e-mail addresses, text messaging or social media must not be used for these communications;

16.1.5 Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies and not to include any unsuitable or abusive material;

16.1.6 Personal information should not be posted on the College website, and only official e-mail addresses will be used to identify members of staff and governors.

16.2 Pupils in the EYFS setting only have access to safe and educational sites and are not left on their own with IT equipment.

Pupils in the EYFS setting are not permitted to bring their own devices into College.

17 Social Media – Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. The College could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the College liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

17.1 The College provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the College through;

17.1.1 ensuring that personal information is not published;

17.1.2 training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues;

17.1.3 clear reporting guidance, including responsibilities, procedures and sanctions;

17.1.4 risk assessment, including legal risk.

17.2 College staff should ensure that;

17.2.1 no reference should be made in social media to pupils, parents/guardians or College staff;
17.2.2 they do not engage in online discussion on personal matters relating to members of the College community;
17.2.3 personal opinions should not be attributed to the College;
17.2.4 security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official College social media accounts are established there should be;

17.2.5 a process for approval by senior leaders;
17.2.6 clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
17.2.7 a code of behaviour for users of the accounts including systems for reporting and dealing with abuse and misuse.

Understanding of how incidents may be dealt with under College disciplinary procedures.

The College's use of social media for professional purposes will be checked regularly.

17.3 Personal Use

17.3.1 Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the College or impacts on the College, it must be made clear that the member of staff is not communicating on behalf of the College with an appropriate disclaimer. Such personal communications are within the scope of this policy.
17.3.2 Personal communications which do not refer to or impact upon the College are outside the scope of this policy.
17.3.3 Where excessive personal use of social media in College is suspected and considered to be interfering with relevant duties, disciplinary action may be taken.

18 Monitoring of Public Social Media

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

18.2 The College should effectively respond to social media comments made by others according to a defined policy or process.

19 Unsuitable/Inappropriate Activities

Some internet activity, e.g. accessing Child Sexual Abuse Material (CSAM) or disturbing racist material is illegal internet activity, and banned from College and all other technical systems. Other activities e.g. cyber-bullying is prohibited and could lead to criminal prosecution. There are however a range of activities which may be, generally, legal but would be inappropriate in the College context, either because of the age of the users or the nature of those activities.

19.1 Misuse of Technology

The College recognises that not all inappropriate use of technology constitutes illegal activity. Incidents such as accessing unsuitable websites, inappropriate online communication, misuse of devices or breaches of the Pupil User Agreement will be addressed proportionately, taking into account the pupil's age, understanding, individual needs and the nature of the incident see **appendix 1 & 2 for examples**.

Where appropriate, responses will focus on education, reflection and restorative approaches, alongside any necessary sanctions in accordance with the College's Behaviour Policy. Any concerns that indicate a potential safeguarding risk will be referred to the DSL and managed in line with the Child Protection Policy.

Further guidance on responding to incidents involving the misuse of technology that do not constitute illegal activity can be found in **Appendix 2.**

19. 2 Illegal Online Activity

The College takes any suspected illegal online activity seriously and will respond promptly in accordance with *Keeping Children Safe in Education (KCSIE) 2026* and relevant legislation.

Where online activity may constitute a criminal offence, including grooming, exploitation, threats, harassment, sharing indecent images of children or the creation and distribution of illegal AI-generated content, the concern must be reported immediately to the Designated Safeguarding Lead (DSL).

The DSL will assess the risk, take appropriate steps to safeguard those involved and determine whether a referral to the police, children's social care or other relevant agencies is required. Where there is immediate danger, the police will be contacted without delay.

Staff must not investigate suspected criminal activity themselves or intentionally view, download, copy or share illegal images. Relevant information should be recorded securely on CPOMS, and any potential digital evidence preserved in accordance with safeguarding procedures and police advice.

The College will ensure that pupils involved in such incidents receive appropriate pastoral and safeguarding support, recognising that children may be victims of exploitation or abuse even where their actions appear to constitute an offence.

All incidents will be managed sensitively, proportionately and in accordance with the College's Child Protection Policy, with appropriate consideration given to confidentiality, information sharing and the protection of all pupils involved, **see Appendix 2.**

19.3 Suspected Illegal Online Activity Involving Staff

The College takes any suspected illegal online activity involving staff, volunteers or contractors seriously and will respond promptly in accordance with *Keeping Children Safe in Education (KCSIE) 2026*, relevant legislation and the College's Child Protection and Allegations Against Staff procedures.

Any concern that a member of staff may have engaged in illegal online activity, including grooming, sexual exploitation, inappropriate sexual communication with children, accessing or sharing indecent images of children, or creating or distributing illegal AI-generated

material, must be reported immediately to the Head. Where the concern involves the Head, it must be reported to the Chair of Governors. **See Appendix 2 for the procedures involved.**

Appendix 1

Examples of how an online incident may be dealt with

Pupils

Whenever a pupil or member of staff infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the ELT. The following are set out as guidance based on the level of infringement.

Example 1

1.1 Use of non-educational sites during lessons.
1.2 Unauthorised use of e-mail.
1.3 Use of unauthorised instant messaging/social networking sites.

Possible sanctions

Referred to class teacher or form tutor for a warning and clarification of what can happen if this is repeated. Conversation with Deputy Head of Prep School, Head of Lower School, Head of Upper School, Head of Sixth Form.

Example 2

1.4 Continued use of non-educational sites during lessons after being warned.
1.5 Continued unauthorised use of e-mail after being warned.
1.6 Unauthorised use of mobile phone (or other new technologies) in lessons e.g. Year 7 to 11 pupils having a mobile phone out of its Yondr pouch during the school day.
1.7 Continued unauthorised instant messaging/chatrooms/social networking sites.
1.8 Use of filesharing software for the purposes of sharing music, games or videos illegally.
1.9 Accidentally corrupting or destroying others' data without notifying a member of staff of it.
1.10 Accidentally accessing offensive material and/or not notifying a member of staff of it.
1.11 Not logging off and/or using other pupils log on details.

Possible Sanctions

Referred to class teacher or Head of Department for follow-up action which could include detention or removal of internet and/or e-mail access for a period of time.

Mobile phone removed from pupil and passed to the relevant Deputy Head of Prep School, Head of Lower School, Head of Upper School, Head of Sixth Form or the Deputy Head (Operations) for collection at the end of the College day.

Use of mobile phones from Yr7 to Yr11 when it should be on your Yondr Pouch will result in removal of the pupils' phone, a phone call home from the relevant Head of Year and a Friday Night detention. The pupil will also be referred to the Online Safety Lead for a warning of what could happen if this is repeated (particularly for the last two situations).

Example 3

1.12 Deliberately corrupting or destroying someone's data, violating the privacy of others.
1.13 Sending an e-mail or text message that is regarded as harassment or of a bullying nature (one-off).
1.14 Deliberately trying to access offensive or pornographic material.
1.15 Any purchasing or ordering of items over the internet (without permission from staff).
1.16 Transmission of commercial or advertising material.

1.17 Deliberately using another pupil's login details for malicious purposes and/or passing out your personal login details to another pupil.

Possible Sanctions

Referred to relevant Deputy Head of Prep School, Head of Lower School, Head of Upper School, Head of Sixth Form or a Deputy Head for a warning and clarification of what can happen if this is repeated and contact with parents as well as removal of internet and/or e-mail privileges for a period of time; referred to the Online Safety Lead for a warning of what could happen if this is repeated (particularly for the last two situations); removal of technological device and parent contacted if this is not done via the College network.

If inappropriate web material is accessed, then ensure the Senior IT Operations Manager is informed and that appropriate technical support filters the site and inform the Deputy Head.

Example 4

1.18 Continued sending of e-mails or text messages regarded as harassment or of a bullying nature after being warned.
1.19 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
1.20 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
1.21 Bringing the College name into disrepute.
1.22 Using the College network as a means of inciting riot or public order offences.
1.23 Deliberately trying to circumvent the IT Security Policy.

Possible Sanctions

Referred to Head of Prep School, Deputy Heads, Head, contact with parents which may include exclusion as well as referral to the Community Police; removal of technological device and parent contacted if this is not done via the College network; contact with the Child Exploitation and Online Protection Unit.

If appropriate, secure and preserve any evidence, for example, print-outs of e-mails/texts and inform the sender's service provider.

Members of Staff

Examples of misconduct

Excessive use of Internet for personal activities not related to professional development, for example, online shopping, personal e-mail, instant messaging, etc.

1.24 Use of personal data storage media (for example, USB memory sticks) without considering access and appropriateness of any files stored.
1.25 Not implementing appropriate safeguarding procedures.
1.26 Any behaviour on the world wide web that compromises the staff member's professional standing in the College and community.
1.27 Misuse of first level data security, for example, wrongful use of passwords.
1.28 Breaching copyright or licence, for example, installing unlicenced software on the network.

Possible Sanctions

Referred to Line Manager/Head and warning given.

Gross Misconduct

1.29 Serious misuse of, or deliberate damage to, any College computer hardware of software.
1.30 Any deliberate attempt to breach data protection or computer security rules.
1.31 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
1.32 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
1.33 Bringing the College into disrepute.

Possible Sanctions

Referred to Head/Governors and follow the College's disciplinary procedures; report to Human Resources/involvement of the Police, if appropriate.

Where a safeguarding concern involves the use of College ICT equipment, immediate steps will be taken to protect pupils and prevent further access to potentially harmful or illegal material.

- Secure the device: The device will be secured to prevent further access or interference. Staff must not investigate, search, download, copy or share suspected illegal material. Any action to preserve digital evidence will be guided by the DSL, IT team and, where appropriate, the police.
- Report and refer**:** Concerns must be reported immediately to the DSL. Where the concern involves a member of staff, it must be reported to the Head, or the Chair of Governors if it concerns the Head. The College will follow its Child Protection and Allegations Against Staff procedures.
- Seek external advice**:** Where indecent images of children or other potentially illegal material are suspected, the College will seek police advice promptly. Where an allegation against a member of staff meets or may meet the harm threshold, the Head will consult the Local Authority Designated Officer (LADO) without delay and within one working day.
- Consider protective measures**:** Appropriate steps will be taken to safeguard pupils while concerns are assessed. Where a member of staff is implicated, suspension will not be automatic but will be considered where necessary and proportionate, following consultation with the LADO and/or police as appropriate.
- Review ICT systems: Where appropriate, the College may commission an independent audit of ICT equipment, filtering and monitoring arrangements to identify potential risks and ensure that appropriate safeguards are in place. Any examination of devices potentially containing criminal evidence will be agreed with the police beforehand.
- Record and review: All concerns, decisions and actions will be recorded securely and confidentially. The College will review any identified safeguarding or technical weaknesses and take appropriate action to prevent recurrence.

All incidents will be managed in accordance with *Keeping Children Safe in Education (KCSIE) 2026*, relevant legislation and the College's Child Protection Policy.

Appendix 2

Procedure for Managing Filtering and Monitoring Alerts

The College uses Securely and other appropriate technical systems to support the filtering and monitoring of online activity. These systems support, but do not replace, effective supervision, safeguarding awareness and professional judgement.
Alerts will be categorised according to the level and nature of risk. Alerts indicating an immediate or serious risk to a child must be sent without delay to the Designated Safeguarding Lead or a deputy through an agreed and reliable communication method. Arrangements will be maintained for receiving and responding to urgent alerts during boarding hours and other College activities outside the normal school day.
The Designated Safeguarding Lead or a deputy will review safeguarding alerts promptly and determine the appropriate response. The response may include:

- checking the pupil's immediate safety and welfare;
- speaking with the pupil in an appropriate and supportive manner;
- reviewing relevant contextual information;
- informing parents or carers where appropriate and safe to do so;
- providing pastoral or safeguarding support;
- making a referral to children's social care, the police or another agency;
- considering whether other pupils may be at risk;
- requesting proportionate technical action; and
- updating relevant risk assessments and support plans.

A safeguarding alert must not be treated solely as a behaviour or disciplinary matter. Where an alert may indicate abuse, exploitation, self-harm, suicide risk, radicalisation, harmful sexual behaviour, the sharing of intimate images or another safeguarding concern, the Designated Safeguarding Lead or a deputy must lead the response.

Staff asked to follow up an alert must report their findings and actions to the Designated Safeguarding Lead. They must not close or downgrade a safeguarding concern without the agreement of the Designated Safeguarding Lead or a deputy.

Lower-level technical or acceptable-use concerns may be delegated to appropriate pastoral or IT staff. If further information suggests that the concern is more serious than first understood, it must be escalated immediately to the Designated Safeguarding Lead or a deputy.

All safeguarding alerts, decisions, conversations, actions and outcomes will be recorded on ~~the~~ CPOMS.

The Designated Safeguarding Lead, responsible Senior Leadership Team member and Senior IT Operations Manager will review patterns and trends in alerts. This information will contribute to the annual filtering and monitoring review, safeguarding training, curriculum planning and decisions about technical controls.

If an alert concerns a member of staff, it must be reported and managed in accordance with the allegations and low-level concerns procedures in the Child Protection Policy and Staff Code of Conduct. The matter must not be investigated solely through the Online Safety Committee or IT department.

Procedures for responding to online safety concerns

The College is committed to providing a safe digital learning environment for all pupils and staff. Any online safety concerns, whether identified during lessons, through the College's filtering and monitoring systems, or involving the conduct of a member of staff, will be taken seriously and responded to promptly, proportionately and consistently.
The College's approach is informed by *Keeping Children Safe in Education (KCSIE) 2026*, the *Online Safety Act 2023*, the *Education Act 2002*, the *Equality Act 2010* and relevant Department for Education guidance on filtering and monitoring.

Online Safety Concerns Identified During Lessons

Where a member of staff identifies an online safety concern during a lesson or supervised school activity, the following procedures must be followed:

1. Immediate intervention: The member of staff must respond promptly to prevent further exposure to harmful or inappropriate content or behaviour. This may include directing the pupil to close a website, stop an online activity or temporarily cease using a device.

2. Assess immediate risk**:** Staff should establish whether the incident presents an immediate safeguarding risk, including exposure to harmful content, cyberbullying, online grooming, sexual harassment, inappropriate contact, extremist material or the sharing of intimate images.

3. Report the concern**:** All safeguarding-related online safety concerns must be recorded promptly on CPOMS and referred to the Designated Safeguarding Lead (DSL) or a Deputy DSL. Urgent concerns must be communicated directly and immediately, rather than relying solely on CPOMS.

4. Preserve appropriate evidence**:** Staff should record relevant factual information, including the website or platform involved, the nature of the concern, the pupils involved and any immediate actions taken. Staff must not download, screenshot, copy or forward nude or semi-nude images of children. Any such incidents must be managed in accordance with KCSIE 2026 and the College's procedures for sharing nudes and semi-nudes.

5. Safeguarding assessment: The DSL will assess the nature and seriousness of the concern, consider the potential impact on the pupil and determine whether further action is required. This may include contacting parents, providing pastoral support, implementing protective measures or making a referral to external safeguarding agencies.
6. Technical response**:** Where the concern relates to access to inappropriate content, the Senior IT Operations Manager and IT team will be informed so that filtering and monitoring arrangements can be reviewed. Any identified weaknesses will be addressed promptly and recorded in the College's Filtering and Monitoring Log.

7. Education and follow-up**:** Where appropriate, the incident will be used as an opportunity to reinforce safe and responsible online behaviour through individual guidance, pastoral support or the PSHE curriculum. Responses will be proportionate to the pupil's age, understanding, needs and circumstances.

8. Review *and* monitoring**:** The DSL and Senior IT Operations Manager will review incidents to identify patterns, emerging risks or areas requiring further staff training, curriculum development or technical safeguards.

Online Safety Concerns Involving Members of Staff

Any concern involving a member of staff's online conduct, including the inappropriate use of technology, online communication with pupils, access to inappropriate material or breaches of professional boundaries, must be addressed in accordance with KCSIE 2026, the College's Staff Code of Conduct, Low-Level Concerns Policy and Allegations Against Staff procedures.

The following steps will apply:

1. Report immediately: Any concern about a member of staff's online conduct must be reported to the Head without delay. Where the concern involves the Head, it must be reported to the Chair of Governors. Staff must not investigate concerns independently or discuss them unnecessarily with colleagues.

2. Ensure immediate safeguarding: Where a pupil may be at risk, appropriate protective measures must be considered immediately. The DSL should be involved in safeguarding arrangements where appropriate, without compromising any investigation or statutory referral process.

3. Determine the appropriate response**:** The Head will assess whether the concern:

    - Constitutes a low-level concern, including conduct inconsistent with the Staff Code of Conduct.
    - Meets, or may meet, the harm threshold for allegations against staff.
    - Requires immediate referral to the police or children's social care because a child may be at risk of significant harm or a criminal offence may have occurred.

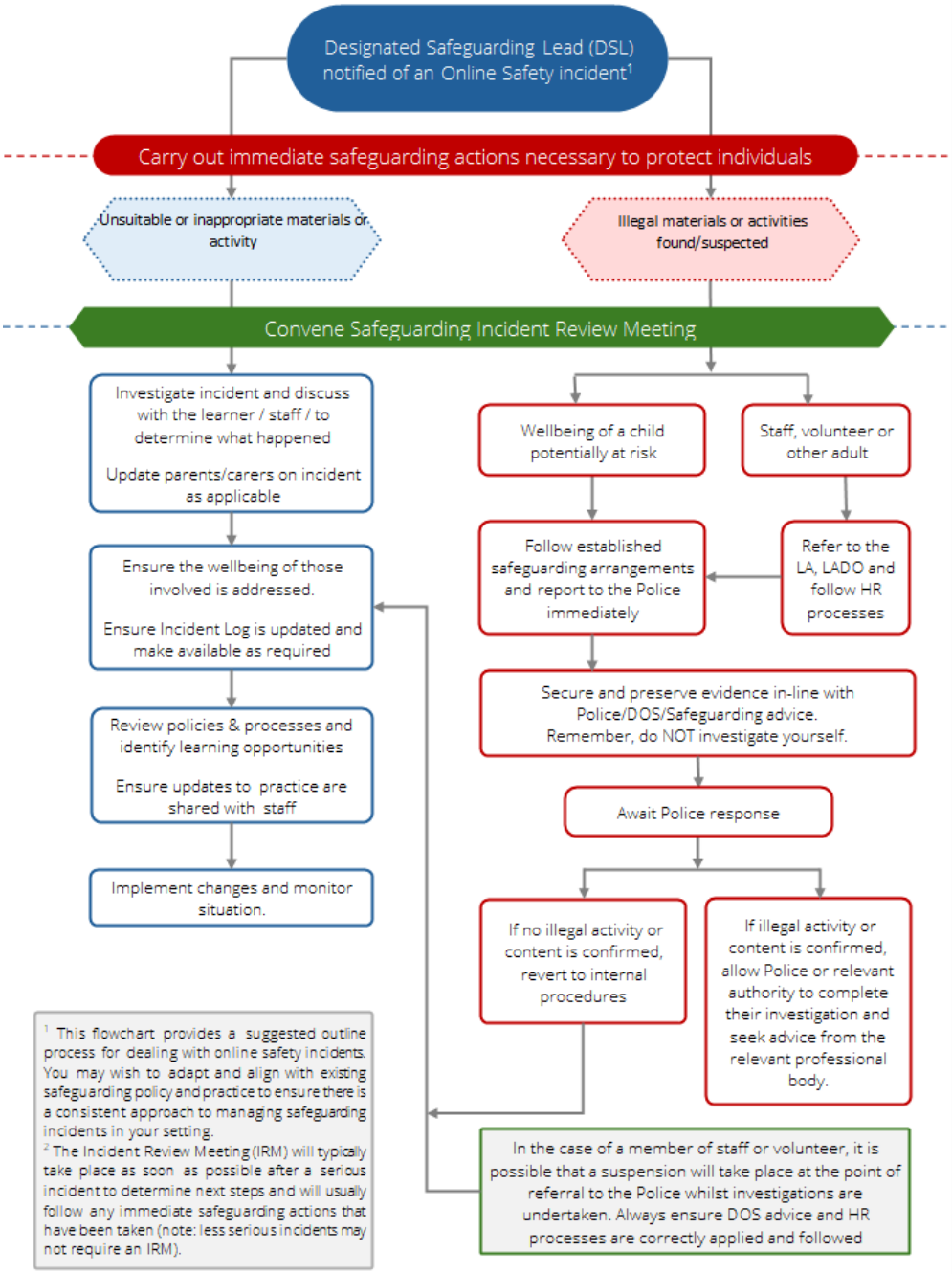
4. Follow statutory procedures**:** Where the harm threshold is met or may be met, the Head will contact the Local Authority Designated Officer (LADO) in accordance with KCSIE 2026 and local safeguarding procedures. The College will not undertake an internal investigation before obtaining appropriate LADO advice.

5. Manage low-level concerns: Concerns that do not meet the harm threshold will be recorded, reviewed and managed in accordance with the College's Low-Level Concerns Policy. Patterns of behaviour will be monitored, and concerns will be escalated where appropriate.

6. Preserve evidence and confidentiality**:** Relevant digital evidence and records must be securely preserved, with access restricted to those who need to know. Staff must not independently search devices or accounts, access private communications without authority, or circulate inappropriate material.

7. Consider external reporting**:** Where appropriate, the College will consult or refer to the police, children's social care, LADO or other relevant agencies. Where statutory criteria are met, the College will fulfil its duty to refer to the Disclosure and Barring Service (DBS) and consider any applicable Teaching Regulation Agency referral.

8. Record and review: All concerns, decisions, actions and outcomes will be recorded securely in accordance with KCSIE 2026 and the College's safeguarding and data protection procedures. Lessons learned will inform staff training, online safety procedures and the ongoing review of filtering and monitoring arrangements.



Oversight and Accountability

The DSL retains overall responsibility for safeguarding responses to online safety concerns, supported by the Senior It Operations Manager, IT team and relevant senior leaders.
The College's Online Safety Committee will review emerging risks, incident trends, filtering and monitoring effectiveness, and developments in technology, including artificial intelligence, generative AI, deepfakes and online communication platforms.
The College recognises that the Online Safety Act 2023 places primary duties on regulated online service providers. Within the school environment, the College will continue to fulfil its own safeguarding responsibilities through appropriate supervision, preventative education, effective filtering and monitoring, staff training and clear reporting procedures.
Online safety concerns will be reviewed regularly to ensure that safeguarding arrangements remain effective, proportionate and responsive to emerging risks.

Appendix 3 – Useful Resources

The following links may help those who wish further information regarding online safety.

UK Safer Internet Centre

Safer Internet https://www.saferinternet.org.uk/advice-centre
South West Grid for Learning - https://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
Thinkuknow https://www.thinkuknow.co.uk/

Others

INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Bullying/Online-bullying/Sexting/Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - Department for Education Cyberbullying: Advice for headteachers and school staff Department for Education –

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Insafe - Education Resources

Parents and Guardians

SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
NSPCC Online Safety https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
Thinkuknow https://www.thinkuknow.co.uk/parents/
Internet Matters https://www.internetmatters.org/advice/
North Yorkshire Safeguarding Children Partnership (NYSCP)
http://www.safeguardingchildren.co.uk/parents-and-carers
Safer Internet http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers DfE Filtering and Monitoring Standards

The 2026 DfE Filtering and Monitoring standards: AI Updates ITs & DSLs Need to Know