



ONLINE SAFETY POLICY

‘This policy will be implemented in a way which honours the vision that every FCJ school is a community of persons - students, staff, governors - bound together in mutual respect and ready to rely on each other in fulfilling their privileged task as educators in a Catholic school.’

Contents

1. Aims	2
1.1 The Four Categories of Risk	2
2. Legislation and Guidance	2
3. Roles and Responsibilities.....	3
3.1 Governing Body.....	3
3.2 Headmistress	3
3.3 Designated Safeguarding Lead.....	3
3.4 Deputy Headteacher (Ethos and Personal Development)	4
3.5 Filtering and Monitoring Responsibilities	4
3.6 All staff, including agency staff, contractors and volunteers	4
3.7 Parents.....	4
3.8 Visitors and members of the community.....	5
4. Educating Pupils About Online Safety.....	5
4.1 Curriculum Integration	5
4.2 Whole-School Reinforcement.....	6
4.3 Reporting and Support.....	6
5. Educating Parents About Online Safety	7
6. Cyber-Bullying.....	7
6.1 Definition	7
6.2 Preventing and Addressing Cyber-Bullying	7
6.3 Searching, Confiscating and Examining Electronic Devices	7
7. Acceptable Use of the Internet in School.....	9
8. Mobile Phones and Personal Smart Technology	9
9. Staff Use of Work Devices and Remote Access Outside School	10
10. Responding to Misuse.....	11
11. Training	11
12. Monitoring Arrangements	12
13. Links with Other Policies	13
Appendix A: Acceptable Use Agreement (Pupils and Parents/Carers).....	14
Appendix B: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)	15

1. Aims

Upton Hall School FCJ aims to:

- maintain robust and proportionate arrangements to promote the online safety of pupils, staff, volunteers and governors
- educate the school community to use technology safely, responsibly, critically and ethically
- protect pupils from harmful content, contact, conduct and commercial risks
- establish clear arrangements for reporting, recording, triaging and responding to online incidents
- maintain effective filtering, monitoring, cyber-security and access-management arrangements
- ensure that emerging technology, including generative artificial intelligence, is used safely and appropriately

This policy applies to the use of school networks, systems and devices. It also applies to online behaviour outside school where it affects the welfare of a pupil, the safety or orderly running of the school, the reputation of members of the school community or relationships between pupils.

1.1 The Four Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content:** exposure to illegal, inappropriate or harmful material, including pornography, misogyny, racism, antisemitism, misinformation, disinformation, content promoting self-harm or suicide, extremist material and content altered or generated using AI.
- **Contact:** harmful interaction with other users, including peer pressure, grooming, coercion, sexual or criminal exploitation, financially motivated sexual extortion, radicalisation and adults posing as children.
- **Conduct:** behaviour that causes or increases the risk of harm, including cyberbullying, abusive or discriminatory messages, impersonation, sexual harassment, making or sharing nudes and semi-nudes, non-consensual recording, misuse of AI and sharing another person's information without permission.
- **Commerce:** risks involving online gambling, financial scams, phishing, inappropriate advertising, in-app purchases, consumer manipulation and financial exploitation.

1. Legislation and Guidance

This policy has been prepared with regard to:

- Keeping Children Safe in Education 2026
- Teaching Online Safety in Schools
- Mobile Phones in Schools: statutory guidance
- Searching, Screening and Confiscation: advice for schools
- Sharing Nudes and Semi-nudes: advice for education settings working with children and young people
- the filtering and monitoring standards for schools and colleges
- the cyber-security standards for schools and colleges
- Relationships and Sex Education and Health Education statutory guidance
- the Prevent Duty guidance

This policy has regard to the following statutory duties and legal framework:

- Education Act 1996
- Education (Independent School Standards) Regulations 2014
- Equality Act 2010
- Children and Families Act 2014
- Counter-Terrorism and Security Act 2015
- Human Rights Act 1998
- data protection legislation, including the UK General Data Protection Regulation, Data Protection Act 2018 and Data (Use and Access) Act 2025
- Children's Wellbeing and Schools Act 2026

The following legislation also informs the school's education about and response to harmful or unlawful online

conduct:

- Computer Misuse Act 1990
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Online Safety Act 2023
- Crime and Policing Act 2026

Some of this legislation creates criminal offences or places duties on online service providers rather than imposing direct duties on the school. It is included because it informs the curriculum, behaviour expectations, risk assessment and the school's response to online incidents.

2. Roles and Responsibilities

3.1 Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headmistress to account for its implementation.

The Governing Body will coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Mrs Micha Woodworth, safeguarding link governor.

The Governing Body will:

- ensure appropriate filtering and monitoring arrangements are in place
- ensure roles and responsibilities for filtering and monitoring are clearly assigned
- receive the findings of the annual filtering and monitoring review
- consider whether arrangements reflect the age and needs of pupils, including those potentially at greater risk of harm
- ensure online-safety education is inclusive and accessible
- receive sufficient information about significant incidents, trends and actions without being given unnecessary personal information

3.2 Headmistress

The Headmistress is responsible for:

- ensuring that this policy is implemented consistently
- ensuring that roles for online safety, filtering, monitoring, cyber security and data protection are clearly assigned
- ensuring that staff receive appropriate training
- ensuring that significant incidents are responded to under the correct school procedure
- authorising members of staff who may search for prohibited items in accordance with the school's Searching, Screening and Confiscation Policy
- ensuring that resources and technical support are sufficient to maintain safe and resilient systems

3.3 Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

The DSL takes lead responsibility for the safeguarding aspects of online safety and has an appropriate understanding of the school's filtering and monitoring arrangements.

The DSL will:

- advise on online incidents that may involve abuse, neglect, exploitation or another risk of harm
- ensure safeguarding incidents are recorded and managed under the Safeguarding and Child Protection Policy
- contribute to the annual filtering and monitoring review

- review relevant filtering and monitoring alerts and trends
- liaise with children's social care, police or other agencies where appropriate
- work with curriculum, pastoral, behaviour, IT and data protection leads
- ensure staff understand when an online incident must be escalated as a safeguarding concern

This list is not intended to be exhaustive.

3.4 Deputy Headteacher (Ethos and Personal Development)

The Deputy Headteacher responsible for Ethos and Personal Development will:

- oversee the planned and progressive online safety curriculum
- ensure that cyberbullying and other online behaviour incidents are addressed through the Behaviour for Learning Policy
- work with the DSL to identify incidents that also require a safeguarding response
- ensure curriculum content responds to emerging risks, pupil voice and incident trends
- ensure teaching is adapted appropriately for pupils with SEND or other additional needs

This list is not intended to be exhaustive.

3.5 Filtering and Monitoring Responsibilities

The Director of Business, DSL and IT Manager, will:

- maintain filtering and monitoring arrangements that meet the school's safeguarding needs
- ensure harmful and inappropriate content is blocked without unreasonably restricting teaching and learning
- ensure monitoring alerts are directed to appropriately trained staff and escalated promptly
- ensure filtering applies to all relevant school-owned devices, networks, users and locations
- maintain appropriate cyber-security, access-management, backup, malware-protection and incident-response arrangements
- maintain records of filtering tests, monitoring incidents, system changes and actions
- support an effectiveness review at least once each academic year
- assess the implications of new services and technology, including generative AI
- report suspected personal data breaches to the Data Protection Officer

The annual review will be led by the DSL with support from the Director of Business and IT Manager. Findings, actions, responsible persons and completion dates will be recorded and reported to the Governing Body.

3.6 All staff, including agency staff, contractors and volunteers

All staff, including agency staff, contractors and volunteers where appropriate, are responsible for:

- understanding and following this policy and the relevant Acceptable Use Agreement
- modelling safe, professional and responsible use of technology
- ensuring pupils follow the relevant acceptable-use expectations
- reporting technical, cyber-security and data protection concerns through the appropriate route
- recording pastoral or safeguarding concerns on CPOMS and speaking directly to the DSL where a concern is urgent
- reporting behaviour incidents through the school's behaviour system
- avoiding unnecessary viewing, copying or forwarding of harmful or illegal content
- challenging harmful online behaviour and maintaining the attitude that it could happen here
- not attempting to investigate a safeguarding or criminal concern themselves.

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the Headmistress of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems

and internet (Appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Parent and carer support - [Childnet International](#)
- Parents are encouraged to download the National Online Safety app, which aims to educate adults in online safety, so that they can help their child make informed decisions and stay safe online. Parents should enrol to Upton Hall using [this link](#).

Parents and carers are expected to support the school's mobile-phone-free arrangements and speak to their child about safe and respectful online behaviour outside school.

The school recognises that it cannot monitor pupils' use of personal devices and home internet services outside school. However, it will respond where online behaviour affects a pupil's welfare or the school community.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

3. Educating Pupils About Online Safety

Online safety education at Upton Hall School FCJ is embedded across the curriculum and delivered through Computing and the Flourish Programme (our whole-school approach to PSHE and RSE). Our approach is proactive, age-appropriate, and responsive to emerging risks, ensuring pupils are equipped to navigate the digital world safely, confidently and in keeping with our Catholic values.

4.1 Curriculum Integration

Specific online safety issues that are covered across the curriculum are:

- generative AI, deepfakes and deep nudes
- recommender systems and persuasive design
- misinformation and verification
- financially motivated sexual extortion
- cybercrime and Cyber Choices
- reporting and removing harmful content
- age restrictions and terms of service
- password security, multi-factor authentication and phishing
- healthy and proportionate use of technology

Online safety is explicitly taught through:

- Computing lessons, which focus on safe use of networks, managing digital identity and passwords, online research skills and awareness of phishing and malware.
- The Flourish Programme, which addresses safe and respectful online relationships, digital consent, the impact of pornography, harmful content, online bullying and image-sharing.
- Religious Education, where themes of human dignity, ethical use of technology and responsible communication are reinforced.

In Key Stage 3, pupils are taught to:

- Use technology safely, respectfully, responsibly and securely, including how to protect their identity and privacy online.
- Recognise harmful content, contact and conduct and understand how to report concerns.
- Reflect on how faith, dignity and respect shape their online interactions.

In Key Stage 4, pupils build on this by:

- Understanding the changing nature of online risks and how to respond appropriately.
- Exploring the consequences of sharing and receiving explicit content (nudes and semi-nudes), online coercion, and digital reputation. Misogynistic or misandrist content, upskirting or coercive control online **are also explored**.
- Recognising the signs of online grooming, abuse and manipulation.

In Key Stage 5, the Flourish curriculum prepares students for adult life by covering:

- Digital literacy and managing digital footprints.
- Healthy online relationships, consent and boundaries.
- Understanding data usage, scams, online fraud and personal security.

By the end of secondary school, pupils will understand:

- That online behaviour should reflect the same high standards expected offline, rooted in respect and responsibility.
- The risks associated with harmful online content and the difficulty of removing material once shared.
- That making or sharing nudes or semi-nudes of anyone under 18, including material altered or generated using AI, may constitute a criminal offence and always requires a safeguarding response by the school. Pupils will understand the importance of consent and the additional harm caused by non-consensual sharing.
- How personal data is collected, shared, and used, and how to manage privacy settings and report misuse.
- How to identify, avoid, and report online bullying, exploitation, abuse and harassment.
- That they are entitled to support and protection, and that speaking up is a strength.
- Pupils will be taught that gaining unauthorised access to accounts or systems, using another person's credentials, creating or distributing malware, denial-of-service activity and altering data without permission may constitute offences under the Computer Misuse Act 1990. Where appropriate, the school may consider Cyber Choices as a preventative or diversionary response.

Teaching will respond to emerging risks and will include generative AI, manipulated images, deepfakes, financially motivated sexual extortion, misinformation, scams, cybercrime, privacy, persuasive design and the impact of recommender systems. Pupils will learn how to verify information, preserve evidence safely, block and report users and access trusted support.

4.2 Whole-School Reinforcement

Online safety is regularly revisited through assemblies, form time, themed weeks such as Safer Internet Day and sessions with external speakers, including police and safeguarding professionals.

Our Flourish curriculum includes up-to-date case studies, real-world scenarios and links to national guidance, supporting understanding across all key stages.

Pupil voice contributes to curriculum planning and helps identify emerging concerns.

4.3 Reporting and Support

Pupils are actively encouraged to speak up if they are worried about anything they encounter online. They can:

- Report concerns via the SpeakUp section of the Thrive Hub VLE.
- Speak to any trusted adult in school, including the Designated Safeguarding Lead or a Deputy DSL.
- Access signposted links for reporting online sexual exploitation and contacting the Police, clearly displayed in form rooms and on the school VLE.

We are committed to ensuring that every pupil knows how to report concerns safely, feels confident they will be taken seriously, and trusts that appropriate support will follow.

Pupils should not forward harmful content to demonstrate what has happened. Where evidence is held on a device, they should tell a trusted adult or the DSL and follow the adult's instructions.

The school will not require a pupil to disclose a password for a personal account except where this is lawful and managed under an authorised procedure.

4. Educating Parents About Online Safety

The school will raise parents' awareness of internet safety in information evenings, letters or other communications, and in information via our website and social media accounts, such as:

- Yondr and phone-free arrangements
- generative AI and manipulated images
- parental controls and privacy settings
- harmful content and recommender systems
- image-based abuse and sexual extortion
- reporting and removal routes
- age restrictions for platforms

General questions should be raised with the relevant pastoral or senior leader. Safeguarding concerns should be reported to the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headmistress.

5. Cyber-Bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour for Learning policy).

A single online incident may not meet the definition of bullying but may still constitute harassment, discriminatory abuse, sexual harassment, threatening behaviour, intimate-image abuse or another serious behaviour or safeguarding concern.

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their form groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see Section 11 for more detail).

Incidents will be considered under the Behaviour for Learning Policy and, where appropriate, the Safeguarding and Child Protection Policy. The school will consider the impact on the pupil, whether conduct has continued outside school, whether other pupils are at risk and whether criminal or data protection issues arise.

The school may take proportionate steps to contain an incident, preserve evidence and support affected pupils. Staff must not unnecessarily view, copy or forward harmful content.

The DSL will consider police or children's social care involvement where an incident indicates a risk of harm or possible criminal activity. A behaviour response must not replace necessary safeguarding action.

6.3 Searching, Confiscating and Examining Electronic Devices

The Headmistress and members of staff authorised by the Headmistress may search a pupil or the pupil's

possessions where the statutory conditions for a search are met. The school's powers to search for prohibited items, including items identified in the school rules, arise principally under the Education Act 1996.

Mobile phones and similar devices may be identified in the school's Behaviour for Learning Policy as items for which an authorised search may be undertaken. Any search must be necessary, proportionate and conducted in accordance with the latest Department for Education guidance on searching, screening and confiscation. The pupil's cooperation should normally be sought before a search is undertaken.

The school may confiscate a mobile phone or other electronic device as a disciplinary sanction where this is reasonable and proportionate. Confiscation under the school's Mobile Phone Policy does not automatically authorise staff to examine the contents of the device.

An authorised member of staff may examine data or files held on a device that has been lawfully confiscated where there is a good reason to do so. A good reason may exist where there are reasonable grounds to suspect that the device or data has been or could be used to:

- cause harm to a person;
- undermine the safe environment of the school or disrupt teaching;
- commit an offence; or
- breach the school's rules.

Staff must not routinely search through a pupil's messages, photographs, applications, social media accounts or cloud-based storage. Where examination may be necessary, consideration must be given to the pupil's privacy, the seriousness of the concern and whether the proposed action is necessary and proportionate.

Where the device or its contents may relate to a safeguarding concern, the member of staff must stop and refer the matter immediately to the DSL or a deputy. The DSL will determine the appropriate safeguarding response and whether advice should be obtained from children's social care, the police or another relevant agency. Wherever possible, a response should be based on what has been reported rather than staff viewing potentially illegal or harmful material.

Staff must not intentionally view, copy, print, forward, share, store or save suspected nudes or semi-nudes, including images created or altered using artificial intelligence. Staff must not ask a pupil to display, share or download such imagery. They must not delete the imagery or ask the pupil to delete it before the DSL has assessed the incident. If imagery is displayed accidentally, the member of staff must close or put down the device, avoid further viewing and report the matter to the DSL immediately.

Any decision that viewing suspected nudes or semi-nudes is unavoidable must be made by the DSL and must meet the exceptional circumstances set out in the UKCIS guidance. The reasons for the decision and the action taken must be recorded.

Where data may constitute evidence of an offence, it must not be deleted. The device should be secured without further examination and advice obtained from the police. Where the material is not suspected evidence of an offence, the Headmistress, DSL or an appropriately authorised senior leader will decide whether it should be deleted, retained or dealt with in another proportionate way.

A record will be made of any search or examination, including the grounds for the action, the staff involved, the outcome, any safeguarding considerations and the subsequent action taken. Parents or carers will normally be informed of a search and its outcome, unless doing so may place a child at risk or prejudice a safeguarding or criminal investigation.

Any searching, confiscation or examination will be undertaken in accordance with the latest DfE guidance on searching, screening and confiscation, the school's Behaviour for Learning Policy, its Safeguarding and Child

Protection Policy and the UKCIS guidance on sharing nudes and semi-nudes.

Any complaint about the searching, confiscation or examination of an electronic device will be considered under the school's complaints procedure.

6. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (Appendices A-C). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of school networks, systems and devices may be filtered, monitored and logged for safeguarding, cyber-security, operational and acceptable-use purposes. Monitoring will be lawful, transparent and proportionate and will be explained through this policy, the Acceptable Use Agreements and relevant privacy notices.

Access to monitoring information will be restricted to authorised personnel. Information will be reviewed only for a legitimate purpose and retained in accordance with the school's retention arrangements.

Users must not attempt to bypass filtering or monitoring through personal hotspots, VPNs, proxy services or other means.

Filtering and monitoring are not substitutes for education, supervision, professional curiosity or appropriate behaviour management. More information is set out in the acceptable use agreements in Appendices A and B.

7. Mobile Phones and Personal Smart Technology

Upton Hall School FCJ is a mobile-phone-free school. The school's detailed requirements are set out in the Mobile Phone Policy, which should be read alongside this policy and the Behaviour for Learning Policy.

Pupils in Years 7-11 who bring a mobile phone or wearable smart technology to school must secure it in their assigned Yondr pouch on arrival. The device must remain secured and inaccessible throughout the school day, including during lessons, registration, movement between lessons, breaktime and lunchtime. Pouches are opened at dismissal.

Personal smart technology includes mobile phones, smartwatches and other personal devices capable of sending or receiving messages or notifications, accessing online services or recording audio, photographs or video.

Sixth form pupils may use mobile phones only at authorised times and in the designated sixth form areas identified in the Mobile Phone Policy. They must not use phones in front of younger pupils. Use during lessons requires the express permission of the member of staff.

The school will consider reasonable adjustments and individual arrangements where access to a device is necessary because of a medical condition, disability, SEND, safeguarding need, caring responsibility or another exceptional circumstance. Any arrangement will identify the purpose, permitted time and location of use.

Parents or carers who need to contact a pupil during the school day must contact the school office on 0151 677 7696. Emergency communication will be managed through the school.

Unauthorised use, filming, photography or audio recording is prohibited. Breaches will be addressed under the Mobile Phone Policy and Behaviour for Learning Policy. Where an incident indicates that a pupil may have suffered or be at risk of harm, staff must inform the DSL and follow the Safeguarding and Child Protection Policy.

The school recognises that pupils may need to show an online concern or evidence held on a device to a member of staff. In such circumstances, the pupil should inform a trusted adult or the DSL. Staff must not unnecessarily view, copy or forward harmful or illegal content.

The school has regard to the statutory Mobile phones in schools guidance issued under section 36 of the

8. Staff Use of Work Devices and Remote Access Outside School

School devices, accounts and systems must be used in accordance with this policy, the Staff Acceptable Use Agreement, the Staff Code of Conduct and the school's data protection and information security requirements. These expectations apply wherever the device or system is being used, including at home, while travelling and during school visits.

Work devices are provided for authorised professional purposes. Staff must not use them for unlawful, inappropriate or commercial activity and must not permit family members or other unauthorised persons to use them.

Staff must:

- protect devices with a strong password, passcode or other security method approved by the school;
- keep passwords and authentication codes confidential and never approve an unexpected multi-factor authentication request;
- lock the screen whenever the device is left unattended;
- store and transport devices securely and avoid leaving them unattended in vehicles or public places;
- install security updates promptly when instructed to do so;
- use only software, applications, browser extensions and services authorised by the school;
- avoid disabling or circumventing security, filtering, monitoring or device management controls;
- use school-approved systems for storing, accessing and sharing school information;
- ensure that conversations, screens and documents containing personal or confidential information cannot be seen or overheard by unauthorised people; and
- securely return the device and any associated equipment when requested by the school or when their employment ends.

Staff must not store school information in personal email accounts, personal cloud-storage services or unauthorised applications. Personal data should not normally be downloaded or retained locally unless this is necessary for an authorised school purpose and appropriate security measures are in place.

Removable media, including USB drives, must not be used to store or transfer school information unless its use has been authorised and the device is encrypted. Staff must not connect unknown or untrusted removable media to a school device.

Staff should avoid accessing confidential school information using unsecured public Wi-Fi. Where remote access is necessary, staff must use the secure access arrangements provided or approved by the school. Staff must not bypass the school's security controls by using personal hotspots, proxy services or virtual private networks unless expressly authorised for a legitimate work purpose.

Where a personal device is exceptionally used for school business, staff must follow the school's approved arrangements. They must not download or retain pupil records, safeguarding information, photographs or other confidential school data on the device. Personal devices must not be used to photograph or record pupils unless this has been expressly authorised for a defined school purpose and the material is transferred to an approved school system and removed from the personal device as soon as possible.

Staff must use their school email account and other approved communication systems when communicating with pupils, parents or carers. They must not use personal email accounts, personal telephone numbers, private social media accounts or unapproved messaging services for professional communication. Any necessary exception must be authorised in advance by a senior leader and appropriately recorded.

Remote meetings, lessons and communications involving pupils must take place through school-approved platforms and in accordance with the Staff Code of Conduct. Staff should maintain appropriate professional boundaries and consider the visibility of their surroundings, other household members and personal information

when using video or audio communication.

Staff must not enter personal, confidential, commercially sensitive or safeguarding information into generative artificial intelligence tools unless the tool has been approved by the school for that purpose and its use complies with the school's data protection requirements. Outputs produced by artificial intelligence must be checked for accuracy, bias, suitability and potential copyright or confidentiality concerns before being used.

Any loss, theft, damage, suspected malware, unauthorised access, accidental disclosure, phishing attempt or other security concern involving a school device, account or school information must be reported to the IT Manager immediately. Where personal data may have been compromised, the Data Protection Officer must also be informed without delay. Where the incident raises a safeguarding concern, it must be reported immediately to the DSL or a deputy through the school's normal safeguarding procedures.

Staff must not attempt to investigate a suspected cyber incident themselves, delete relevant evidence or conceal an accidental breach. The device should be disconnected from external networks where advised and preserved for examination by authorised personnel.

The school may monitor the use of its devices, accounts and systems for safeguarding, security, operational and compliance purposes. Monitoring will be lawful, necessary and proportionate and will be undertaken in accordance with the school's privacy notices and data protection obligations.

Concerns about the security or appropriate use of a work device should be referred to the IT Manager. Concerns about professional conduct, communication with pupils or online safeguarding must be referred to the Headmistress, DSL or another appropriate senior leader.

9. Responding to Misuse

Online incidents may require one or more of the following responses:

- pastoral: education, support or restoration
- behaviour: a breach of school rules or acceptable use
- safeguarding: a child may have suffered or be at risk of harm
- criminal: an offence may have been committed
- cyber security or data protection: systems or personal information may have been compromised
- staff conduct: the Staff Code of Conduct or professional standards may have been breached

The response will be proportionate to the nature, context and impact of the incident. A behaviour response will not replace safeguarding action where a child may be at risk.

Safeguarding concerns will be managed by the DSL under the Safeguarding and Child Protection Policy. Behaviour matters will be managed under the Behaviour for Learning Policy. Staff conduct matters will be referred to the Headmistress. Cyber-security and data incidents will be referred to the IT Manager, Director of Business and Data Protection Officer as appropriate.

Police involvement will be considered where there is evidence of a crime, immediate risk or significant harm. Staff must not investigate criminal or safeguarding concerns themselves.

10. Training

All new staff members will receive training, as part of their induction on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are

- at risk of online abuse.
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages.
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
 - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will include:

- the school's filtering and monitoring arrangements
- how alerts and blocked-content concerns are escalated
- generative AI and manipulated images
- making and sharing nudes and semi-nudes
- sexual extortion
- cybercrime and Cyber Choices
- data breaches and phishing
- the mobile phone policy
- not viewing or forwarding illegal content

Training will help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will receive training that supports their lead responsibility for online safety and their understanding of filtering and monitoring. Their knowledge will be updated regularly and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

11. Monitoring Arrangements

The DSL will maintain oversight of safeguarding incidents involving online harm through CPOMS.

Behaviour incidents will be recorded through the school's behaviour system.

Filtering and monitoring tests, alerts, incidents, actions and system changes will be recorded by the DSL.

Cyber-security and personal-data incidents will be recorded through the appropriate technical and data-protection processes.

The DSL will lead an annual review of filtering and monitoring with the Director of Business and IT Manager. The Governing Body will receive an appropriate summary of findings, trends, risks and actions.

Curriculum provision will be reviewed in response to pupil voice, incident patterns, emerging technology and national guidance.

This policy will be reviewed annually and following any significant incident or relevant change in

legislation or statutory guidance.

12. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour for Learning Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT policy
- Social media policy

Appendix A: Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's IT systems (like computers) and get onto the internet in school I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell trusted adult immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a staff member
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Use VPNs, proxies, personal hotspots or other methods to bypass controls
- Create or share harmful AI-generated or manipulated content
- Photograph, film or record another person without permission
- Access another person's account or use their credentials
- Attempt to interfere with school systems
- Share nudes or semi-nudes
- Forward harmful material to show another person
- Use unauthorised AI services or submit AI work as my own
- Use mobile phones or wearable technology contrary to the Mobile Phone Policy

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's IT systems and internet. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, the school's policy on Mobile Phones, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix B: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable)

I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teacher's first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will:

- use only authorised software, AI and cloud services
- protect accounts using multi-factor authentication
- report phishing, loss, compromise or data breaches immediately
- not bypass filtering or monitoring
- not use personal accounts to communicate with pupils
- not store school information on unauthorised personal devices
- not enter confidential information into public AI systems
- not photograph, film or record pupils unless authorised
- not view, copy or forward suspected illegal images
- follow the Staff Code of Conduct when using social media

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix C: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	