Online Safety Policy

Rewritten October 2025 **Review Date:** October 2026

1.0 Aims

1.1 Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Comply with all statutory guidance, particularly *Keeping Children Safe in Education (KCSIE)*, regarding filtering and monitoring standards.

1.2 Our approach to online safety is based on addressing the following 4 key categories of risk (The 4 Cs):

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation & conspiracy theories, **and harmful viral challenges/trends.**
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography) **(Sexting)**, sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.3 This policy applies to all members of the school community who have access to and are users of school ICT systems, **and to online behaviour out of school that is linked to membership of the school.**

2.0 Roles and Responsibilities

2.1 **Governors (Online Safety Governor):**

- Responsible for the approval and monitoring of this policy and holding the Headteacher to account for its implementation.
- The Online Safety Governor meets regularly with the OSO, monitors incident logs and filtering/change control logs, and reports to the relevant Governors meeting.
- Governors ensure online safety is embedded in the whole school approach to safeguarding and related policies.

2.2 **Headteacher and Senior Leadership Team (SLT):**

- The **Headteacher** is responsible for ensuring staff understand and implement this policy consistently. (Day-to-day responsibility is delegated to the OSO).
- **SLT** is responsible for ensuring the OSO and DSL receive suitable, up-to-date training.
- The Headteacher and School Business Manager manage procedures for serious online safety allegations against staff or community members.

2.3 **Online Safety Officer (OSO):**

- **Statutory Requirement:** Puts in place an appropriate level of security protection procedures, such as **filtering and monitoring systems (KCSIE)**, which are regularly reviewed to assess effectiveness.
- **Technical Management:** Ensures the school's ICT systems are secure, protected against viruses and malware, and regularly updated. Blocks access to potentially dangerous sites and prevents the downloading of dangerous files.
- **Incident Management:** Ensures all online safety incidents are logged and dealt with in line with this policy and ensures staff are aware of reporting procedures (Beacon Button).
- **Governance:** Reports termly to the SLT and meets regularly with the Online Safety Governor.
- **Access Control:** Ensures networks and devices are accessed via a properly enforced password protection policy (see Technical Security Policy).
- **Bring your own device (BYOD) Verification: Oversees the verification process for BYOD devices (if applicable) to ensure up-to-date antivirus/anti-malware is used.**

2.4 **Designated Safeguarding Lead (DSL):**

- **Statutory Requirement:** Has overall responsibility for Safeguarding and Child Protection, including online safety.
- **Monitoring: Understands the filtering and monitoring systems and processes in place and is responsible for checking relevant reports from monitoring systems and responding to safeguarding concerns identified by the systems.**
- **Training:** Maintains regular and appropriate training to understand the unique risks associated with online safety, including for pupils with **SEND**, and the specific risks of **sexting** and **online radicalisation.**
- **Liaison:** Manages all online safety issues/incidents in line with the safeguarding policy and liaises with external agencies (e.g., Police, Children's Services) where necessary, particularly regarding **illegal images or online radicalisation.**

2.5 **Teaching, Support Staff and Volunteers:**

- Maintain an understanding of and consistently implement this policy.
- **Receive mandatory annual safeguarding and online safety training.**
- Review and adhere to the Acceptable Use Agreement annually.
- Use official school systems for digital communications with students/parents.
- **Monitor the use of digital technologies, mobile devices, cameras, and emerging platforms (e.g., gaming, livestreaming) in lessons.**

2.6 **Students:**

- Responsible for using digital systems according to the **Student Acceptable Use Agreement (AUA).**
- **Understand the importance of reporting abuse, misuse, or access to inappropriate materials via the BCS Beacon Button or to a staff member.**
- Understand policies on mobile devices, digital cameras, and cyber-bullying, and that this policy covers their actions out of school if linked to school membership.

3.0 Education and Training

3.1 **Students:**

- Online safety education is a planned, progressive curriculum integrated into **Computing, PHSE, and other subjects** (e.g., media literacy, critical evaluation).
- Students are taught to be critically aware of online content, validate information, and respect copyright.
- **Online Challenges/Trends:** Students will be educated about the risks of **online challenges and viral trends** and the importance of critical thinking before participating or sharing.
- **Online Gaming:** Guidance covers **age ratings (e.g., PEGI), in-game chat risks, and appropriate platform usage.**
- **Livestreaming:** Education addresses the risks associated with **livestreaming on platforms like TikTok, Twitch, and Instagram Live** (e.g., privacy, contact risks).
- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues (**Prevent duty**).
- **Email Use:** Primary & Middle school students have blocked external email. Upper School students have external email access limited by a regularly reviewed whitelist for activities like university applications.

3.2 **Parents/Carers:** The school provides information and awareness to parents/carers through newsletters, the Parent Zone, campaigns (e.g., Safer Internet Day), and links to external resources (e.g., SWGfL, Childnet).

3.3 **Generative Artificial Intelligence (AI):**

- **Acceptable Use:** The school recognises AI's potential to support learning. **Specific examples of acceptable AI use will be communicated (e.g., Students in Year 5+ may use AI tools to help plan essays but must acknowledge this). Currently student access to known AI chatbots is blocked.**
- **Referencing: AI-assisted work must be referenced/acknowledged** according to departmental guidelines to avoid plagiarism.
- **Age Guidelines:** Guidelines for acceptable AI use are **age-appropriate** (e.g., Year 3 vs Year 11).
- **Detection & Risks:** Students are taught about the risks of AI (misinformation, bias, plagiarism, **AI image generation, and deepfakes**). Staff receive training on managing and detecting AI-generated content.

4.0 Cyber-bullying

4.1 **Definition:** Repetitive, intentional harming of one person or group by another online (social networking, messaging, gaming), involving an imbalance of power.

4.2 **Preventing and Addressing:**

- Pupils are taught what cyber-bullying is and how to report it (as a victim or witness) using the **BCS Beacon Button.**
- **Staff receive training** on cyber-bullying, its impact, and ways to support pupils as part of safeguarding training.
- The school follows the Behaviour Policy for incidents. The DSL will consider reporting illegal material (e.g., threats, extreme pornography) to the Police.

4.3 **Examining Electronic Devices:**

- **Authorised staff (Headteacher, DSL, OSO, SLT)** may search and confiscate a device based on reasonable grounds for suspicion of harm, rule-breaking, or evidence of an offence.

- Searches and examination of data follow the DfE guidance on screening, searching, and confiscation.
- **Searching Protocol:** Searches should be conducted by **two members of staff (safeguarding best practice)** and, where possible, by staff members of the **same gender** as the student being searched.
- **Parental Notification: Parents/carers will normally be informed when a device is confiscated and will be asked to collect the device with their child at the end of the school day.**
- **Critical Protocol for Illegal Content (Sexting/CSAI):** If a staff member suspects or finds an indecent image of a child (including youth-produced sexual imagery or "nudes and semi-nudes"), they will:
    - **Not view the image.**
    - **Stop the search immediately.**
    - **Confiscate the device and report the incident to the DSL immediately.**
    - The DSL will manage the incident according to the school's Safeguarding/Child Protection policy and UKCIS guidance on sharing nudes and semi-nudes. **The material will NOT be deleted if it constitutes evidence relating to a suspected offence, and the Police will be contacted as soon as reasonably practicable.**

4.4 **Off-Site Incidents:** The school has the authority (Education and Inspections Act 2006) to regulate student behaviour off-site when related to school membership. The school deals with such incidents in line with this policy and informs parents/carers where appropriate.

5.0 Technical – Infrastructure / Equipment, Filtering and Monitoring

5.1 The school is responsible for ensuring the infrastructure/network is as safe and secure as possible, implemented through the **Technical Security Policy.**

5.2 **Monitoring:** School technical staff regularly monitor and record user activity. Users are aware of this through the AUA. The filtering system (Chrome extension) is applied automatically via school login and cannot be bypassed on school Chromebooks.

5.3 **Reporting:** The **BCS Beacon Button** is available to all staff, students, and parents for anonymous reporting of technical incidents, security breaches, or online safety concerns.

5.4 **Security:** All staff devices and phones in school should be password protected. Security incidents are reported via safeguarding procedures or the Beacon Button.

5.5 **Guest Access:** Restricted guest access is in place and monitored by the IT Manager.

5.6 **Remote Use:** Staff may use school devices out of school provided the device is protected with up-to-date viral protection and is password protected.

5.7 **Executable Files:** Staff may only download approved executable files from a secure webpage; others must be checked by the OSO first.

5.8 **Removable Media:** Media should be encrypted, stored securely in school, and only used when necessary, with movement towards cloud storage encouraged. Personal data taken off-site must be securely encrypted.

6.0 Use of Digital and Video Images

6.1 The school recognizes the benefits of digital imaging but also the risks (e.g., cyber-bullying, long-term harm from publication).

6.2 **Risk Management:**

- Written permission is obtained before student photographs are published on the school website/social media/local press.
- **Parents/carers** may take videos and digital images at school events for personal use but **must not publish them or comment on other students** on social media to respect privacy and protection.
- Staff/volunteers are allowed to take educational images only on **school equipment**, unless specific SLT permission is granted for a personal device, and the images are promptly transferred and deleted.
- Students must not take, use, share, publish, or distribute images of others without permission.
- Students' full names will **not** be used in association with photographs published online.

7.0 Communication Technologies and Acceptable Use

7.1 **Mobile Devices and Media Use:**

The table below outlines the policy for mobile phones, smartwatches, and other personal digital devices brought onto the school site.

Activity/Device	**Staff & Other Adults**	**Students**	**Policy Notes & Rationale (KCSIE/Safeguarding)**
Mobile phones (kept in bags/off)	Allowed	Allowed	Must be **switched off and kept out of sight** in bags at all times during the school day. Exceptions require Headteacher/DSL approval (e.g., medical reasons).
Smart Watches (internet/phone enabled)	Allowed	Not allowed to be internet enabled	Must be **switched off and kept out of sight.** Smartwatches capable of photo/video, internet access, or communication are not permitted during examination periods (pupils and staff) or during the

			school day (pupils)
Use of mobile phones in lessons / Office work	Staff with Permission	Not Allowed	Staff: Permitted only for educational or essential professional use.
Use of mobile devices in social time	Allowed (Personal)	Not Allowed	**Students:** Must remain off and stored securely. **Staff:** Personal use must not disrupt supervision or bring the school into disrepute.
Taking photos/video on personal devices	Not Allowed	Not Allowed	**Strictly Not Allowed.** Staff must use school-owned equipment (Section 6.2). Students are never permitted to take photos/videos during school time unless explicit staff permission is given for a safe, non-identifying purpose.
Use of other mobile devices (tablets, gaming)	Allowed for Teaching	Not Allowed	Personal gaming devices are banned. Personal tablets (BYOD) may be allowed only with specific subject teacher/SLT permission for educational tasks and must adhere to filtering standards.

7.2 **Email and Messaging:**

Activity/System	**Staff & Other Adults**	**Students**	**Policy Notes & Rationale (Safeguarding/GDPR)**
Use of personal email on school network	Not Allowed	Not Allowed	All communication must use the official, monitored school email service.
Use of school email for personal emails	Not allowed	Not Allowed	Staff and Students: School email is for educational use only.
Use of messaging/chat apps	Not Allowed	Not Allowed	Messaging apps (e.g., WhatsApp, Telegram) must **NOT** be used for communication between staff and students or parents/carers. Only official, monitored school systems are permitted.
Use of social media (Personal Accounts)	Not Allowed (During Work)	Not Allowed	Staff must not access personal social media during working hours unless on a designated break. Students must not access social media on school systems.

Use of blogs/video broadcasting (educational)	Acceptable	Acceptable	Allowed only when directly related to a teaching/learning activity and managed/monitored by staff on school-approved platforms (e.g., Google Classroom, official school YouTube).

7.3 **Communication Practice and Conduct:**

- The official school email service is monitored. Users should only use school email to communicate with others when in school or on school systems.
- Users must immediately report any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying, and **must not respond** to such communication.
- Any digital communication between staff and students or parents/carers must be **professional in tone and content**. These communications **may only take place on official (monitored) school systems**. Personal email addresses, text messaging, or personal social media must be avoided.
- **Staff must ensure:**
  - **No reference is made on personal social media** to students, parents/carers, or school staff that could breach confidentiality.
  - They **do not engage in online discussion on personal matters** relating to members of the school community.
  - Personal views are not attributed to the school.
  - Staff remain aware that personal views expressed on personal social media are public and must **not bring the school into disrepute** (Staff Code of Conduct).
  - **Security settings on personal social media profiles are regularly checked** to minimise risk.
- Whole class/group email addresses will be used at KS1; KS2 and above will have individual school email addresses for educational use.

8.0 Unsuitable / Inappropriate Activities (High-Risk Activities)

8.1 Any internet activity that is illegal (e.g., accessing child abuse images, distributing racist material, **promoting terrorism/extremism**) is banned from school systems. Appropriate action will be taken, including referral to the Police where necessary.

8.2 The school believes the activities below are inappropriate in a school context. Users must

NOT engage in these activities in or outside the school **when using school equipment or systems, or in any way that relates to their membership of the school**.

8.3 High-Risk Online Activities

Activity	Staff & Other Adults	Students	Status (KCSIE/Legal Risk)
Online Gaming (Educational)	Acceptable	Acceptable	Only when directly supervised or assigned for learning purposes.
Online Gaming (Non-Educational)	Unacceptable	Unacceptable	**Banned on school premises/systems .** Risks associated with age ratings (PEGI), in-game chat, and contact risks are covered in the curriculum (Section 3.1).
Livestreaming & Viral Challenges	Unacceptable	Unacceptable	Banned on school systems/premises. Any student involvement in **online challenges or viral trends** that risks physical safety, mental health, or brings the school into disrepute will result in disciplinary action.
Online Gambling	Unacceptable	Unacceptable	**Banned.**

Online Shopping / Commerce	Unacceptable	Unacceptable	Banned on school systems/time (applies to both staff and students).
File Sharing (Non-Educational P2P)	Unacceptable	Unacceptable	Banned due to copyright infringement and network security risk.
Use of Social Media (Educational)	Acceptable	Acceptable	Only on monitored, school-approved accounts/platforms for specific learning objectives.
Use of Video Broadcasting (e.g. YouTube)	Acceptable	Acceptable	Acceptable for educational purposes, but must adhere to filtering and monitoring protocols.
Creating or propagating viruses/harmful files	Unacceptable	Unacceptable	**Banned.**
Infringing copyright	Unacceptable	Unacceptable	**Banned.**

8.4 Illegal and Highly Inappropriate Content (Zero Tolerance)

Users shall not visit Internet sites, make, posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

Activity/Content	**Staff & Other**	**Students**	**Sanction / Action**

	Adults		
Child Sexual Abuse Images (CSAI)	**X Unacceptable**	**X Unacceptable**	**Referral to Police / DSL immediately.** Statutory duty to report.
Grooming, Incitement, Arrangement of Sexual Acts	**X Unacceptable**	**X Unacceptable**	**Referral to Police / DSL immediately.**
Possession of Extreme Pornography	**X Unacceptable**	**X Unacceptable**	**Referral to Police / DSL immediately.**
Criminally racist material / Promotion of religious hatred	**X Unacceptable**	**X Unacceptable**	**Referral to Police / DSL / Disciplinary Action.**
Promotion of extremism or terrorism (Prevent)	**X Unacceptable**	**X Unacceptable**	**Referral to DSL / Prevent Lead immediately.**
General Pornography (Non-Illegal)	**X Unacceptable**	**X Unacceptable**	**Major Disciplinary Action / Referral to Police.**
Threatening behaviour or promotion of physical violence	**X Unacceptable**	**X Unacceptable**	**Major Disciplinary Action / Referral to Police.**
Revealing confidential or proprietary information	**X Unacceptable**	**X Unacceptable**	**Major Disciplinary Action / Staff Disciplinary.**

Using systems to bypass filtering/safeguards	**X Unacceptable**	**X Unacceptable**	**Disciplinary Action / Loss of Access.**
Any material that brings the school into disrepute	**X Unacceptable**	**X Unacceptable**	**Disciplinary Action.**

9.0 Responding to Incidents of Misuse

9.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services, ensuring a safe and secure approach to incident management. Incidents might involve illegal or inappropriate activities (see Sections 8.3 and 8.4).

9.2 **Illegal Incidents (Including Sexual Imagery/Grooming):**

Incident Type	**Immediate Action (Non-Negotiable)**	**Referral**
Suspected Child Sexual Abuse Images (CSAI), Extreme Pornography, or Grooming Behaviour.	**Stop the investigation immediately.** Do NOT view, copy, or forward the image/material. Isolate the device.	**DSL (Designated Safeguarding Lead) and/or Police immediately.**
Other suspected illegal activity (e.g., criminally racist material, promotion of terrorism/extremism, sending obscene materials).	Secure the evidence (e.g., secure screenshot/URL on an investigation machine).	**DSL and Police.**

9.3 **Procedure for Investigating Non-Illegal Incidents:**

In the event of suspicion regarding a policy infringement (careless, irresponsible, or deliberate misuse), the following steps should be followed:

- **Involve multiple senior staff: Have more than one senior member of staff involved** in the investigation process to protect individuals from subsequent false accusations.

- **Designated Investigation Computer:** Conduct the procedure using a **designated computer** that is separate from normal school IT use and can be taken off-site by the police if required.
- **Evidence Collection:** Record the URL of the site and describe the content. **Screenshots may be recorded and stored on the investigation machine, then printed, signed, and attached to the form (except in the case of CSAI – see 9.2).**
- **Judgement:** The staff group will judge whether the concern has substance. If confirmed, appropriate action will be required (Section 10.0).
- **Preservation of Evidence: Isolate the computer in question immediately.** Any change to its state may hinder a later police investigation.
- **Documentation:** All steps must be taken to provide an evidence trail for the school and police, demonstrating that visits to these sites were carried out for safeguarding purposes. The completed form should be retained for evidence and reference purposes.

10.0 School Actions & Sanctions

10.1 **Artificial Intelligence (AI):** The school will treat any use of AI to bully pupils (e.g., through 'deepfakes' that create hoax images, audio, or video) in line with our Anti-Bullying and Behaviour policies. Staff using new AI tools for school purposes must carry out a risk assessment.

10.2 **Proportionate Response:** Incidents will be dealt with as soon as possible, in a **proportionate manner**, through normal behaviour/disciplinary procedures. The tables below outline the escalation paths.

Student Incidents: Escalation and Action Table

Incident Category	Who Decides (Initial)	Escalation Level	Sanctions (Possible)	Technical Action	Inform Parents
1. Deliberate illegal access/CSAI/Grooming (Sec 8.4)	DSL / Headteacher	**Police / LA**	Suspension / Exclusion	Network Access Removal / Device Isolation	**Immediately**
2. Accessing/sharing pornography or promoting extremism	DSL / Headteacher	DSL / Police	Exclusion / Police Referral	Network Access Removal	Immediately

3. Cyber-Bullying / Offensive Message / Harassment	Head of Year / DSL	DSL / Headteacher	Warning / Detention / Exclusion	Network Access Removal	Yes
4. Unauthorised use of mobile phone/social media/filtering subversion	Class Teacher / Head of Dept.	Headteacher	Warning / Detention / Loss of Device/Access	Network Access Removal / Filtering Action	Yes
5. Password sharing / Attempting account access (Student/Staff)	Head of Dept.	Headteacher	Warning / Detention / Suspension	Network Access Removal	Yes
6. Corrupting data / Deliberate hardware damage	Head of Dept.	Headteacher	Detention / Suspension / Exclusion / Cost Recovery	Technical Support	Yes
7. Accidentally accessing inappropriate material and *failing to report*	Class Teacher / Head of Dept.	DSL	Warning / Detention	Filtering Review	Yes
8. Actions bringing the school into disrepute (off-site)	Head of Year / DSL	Headteacher	Warning / Detention / Suspension	N/A	Yes

Escalation Levels:

- **Warning:** Recorded by Class Teacher/Head of Dept.
- **Headteacher:** Leads investigation, determines detention/suspension/exclusion.

- **DSL/Police/LA:** Used when safeguarding is primary concern, or criminal activity is suspected.

Staff Incidents: Escalation and Action Table

Incident Category	Who Decides (Initial)	Escalation Level	Disciplinary Action	Technical Action
1. Deliberate illegal access/CSAI/Grooming	Headteacher	**Police / Local Authority**	Suspension / Referral for Dismissal	Network Access Removal / Device Isolation
2. Digital communication with students via non-school systems (e.g., personal text/social media)	Line Manager	Headteacher / LA	Warning / Disciplinary Action / Suspension	N/A
3. Deliberate breach of Data Protection / Network Security / Destroying data	Headteacher	Headteacher / LA	Warning / Suspension / Disciplinary Action	Technical Support
4. Sending offensive/harassing message or Corrupting data	Line Manager	Headteacher / LA / Police	Warning / Suspension / Disciplinary Action	Technical Support
5. Inappropriate personal use of internet/social media/filtering subversion	Line Manager	Headteacher	Warning / Disciplinary Action	Technical Support
6. Careless use of personal data / Sharing passwords	Line Manager	Headteacher	Warning / Disciplinary Action	Technical Support

7. Actions compromising professional standing or bringing school into disrepute	Line Manager	Headteacher	Warning / Disciplinary Action / Suspension	N/A

11.0 Review of this Policy

11.1 In writing this policy Bradford Christian school acknowledges:

- The materials supplied and used from SWGfL Online Safety School Template Policies
- The Education and Inspections Act 2006
- **The Education Act 2011**
- **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**
- **Keeping Children Safe in Education (KCSIE) 2025**
- Equality Act 2010
- **The DfE Cyber Security Standards for Schools and Colleges**

11.2 This policy should be read in conjunction with the following school policies:

- **Technical Security Policy**
- Data Protection Policy
- Behaviour and Discipline Policy (students)
- Discipline Policy (staff)
- **Safeguarding and Child Protection Policy (especially for Sexting/CSAI protocols)**
- **Preventing Extremism and Radicalisation Policy**
- Anti-Bullying Policy
- Staff Code of Conduct
- Complaints Policy
- Privacy Notices

12.0 Version Control

Date of Adoption of this Policy	17 December 2025
Date of last review of this policy	November 2024
Date of next review of this policy	October 2026
Policy Owner (SLT)	Jane Prothero
Policy Owner (Governors)	Adetola Ayenitaju

Bradford Christian School - Student Acceptable Use Agreement (AUA)

Our Commitment to Safe Technology Use

I understand that I must use the school's ICT systems, network, internet access, and devices in a **responsible, safe, and legal way**. I agree to abide by the school's **Online Safety Policy** and **Technical Security Policy** at all times.

1. My Account and Security Responsibilities

1.1 **Passwords:** I will **always keep my username and password secure** and will **never share them** with anyone else. I understand that I am responsible for all activity that occurs under my account. 1.2 **Device Safety:** I will keep my school-issued devices (e.g., Chromebook) safe, protected from damage, and will report any loss or damage immediately to a teacher. 1.3 **Access:** I will **not attempt to access, or use,** the account, files, or data belonging to another student or staff member. 1.4 **Monitoring:** I understand that my use of the school network is **monitored and logged** for my safety and the security of the school.

2. Appropriate Use and Content (The 4 Cs)

2.1 **Educational Use:** I will only use the school's ICT systems and the internet for **educational purposes** as directed by a teacher. 2.2 **Bypassing Safety:** I will **never attempt to bypass the school's filtering or security systems** (e.g., by using proxy sites or unauthorized software). 2.3 **Illegal/Harmful Content:** I understand that I must **never attempt to access, download, view, or share** any illegal, inappropriate, or harmful content, including: * Pornography or illegal sexual images (CSAI, Grooming). * Content that promotes **extremism, terrorism, racism, hatred, or violence.** 2.4 **Copyright:** I will respect copyright and intellectual property when using material accessed online. 2.5 **Prohibited Activities:** I will not use the school network or devices for **online gambling, shopping/commerce, or non-educational file-sharing.**

3. Communication, Conduct, and Respect

3.1 **Cyber-bullying:** I will treat all users (students and staff) with respect. I will **not use ICT systems to bully, harass, threaten, or insult** others. This includes the use of **deepfakes or AI-generated content** to impersonate or defame others. 3.2 **Professional Contact:** I will **only use official school communication systems** (e.g., school email, Google Classroom) for contact with staff. **I must never communicate with staff via personal email, text message, or social media.** 3.3 **Online Challenges:** I will **not participate in online challenges or viral trends** that pose a risk to physical safety, mental health, or that could damage the school's reputation.

4. Mobile Devices and Images

4.1 **Mobile Phones:** My personal mobile phone and smartwatch must be **switched off and kept out of sight** in my bag during the school day. I will only use a personal device if **explicitly permitted by a member of staff** for a specific learning activity. 4.2 **Taking Images:** I will **never take, use, share, publish, or distribute images, videos, or audio recordings of any other person** (student or staff) without their explicit permission and the permission of a teacher.

5. Reporting Incidents (The BCS Beacon Button)

I know the importance of reporting concerns immediately. If I encounter any inappropriate material, receive an uncomfortable message, or witness misuse:

1. I will **not respond** or attempt to hide the material.
2. I will immediately report the incident to a trusted member of staff (teacher, Head of Year, DSL).
3. I know I can use the **BCS Beacon Button** for anonymous reporting of a concern.

I have read and understood the terms of this Acceptable Use Agreement. I agree to comply with these rules and understand that failure to do so may result in sanctions, including loss of network access, detention, suspension, or exclusion.

Student Signature: _____

Parent/Carer Signature: _____

Date: _____

Online Safety Incident Reporting Flowchart

This chart covers incidents reported by students, staff, or monitoring systems.

Phase 1: Immediate Discovery & Assessment

Step	Action	Decision Point
1.	**Staff member becomes aware of an incident** (Observed, Reported by student/parent, Flagged by monitoring system/Beacon Button).	**Is the child/staff member in immediate danger, or does the incident involve illegal content (CSAI, Grooming, Extreme Pornography, Threat to Life, Extremism)?**
2.	**Secure the Scene & Evidence (DO NOT VIEW/DELETE)** *If in school, take control of the device. Do NOT turn it off or delete files. If on screen, turn off the monitor or minimize the window.*	**YES (High Risk)**

Phase 2: High-Risk (Illegal/Safeguarding) Incidents

Step	Action
3.	**STOP THE INVESTIGATION IMMEDIATELY. Do NOT copy, view, or forward the illegal material.** (Viewing or copying CSAI may constitute an offence).
4.	**Alert DSL Immediately.** If the DSL is unavailable, contact the Deputy DSL or Headteacher. **The DSL takes over the investigation.**

5.	**DSL Action Isolate the computer/device.** The DSL/Headteacher assesses the risk of **Significant Harm**. If confirmed, or if the content is CSAI/Grooming: **Referral to Police and/or Local Authority Children's Services.** (See Section 9.2).
6.	**Secure Evidence** The device is secured for potential Police examination (Section 4.3). All actions, including the referral, are documented in the safeguarding system (e.g., CPOMS).
7.	**Police/LA Action** School follows all instructions from the Police or Children's Services. Internal disciplinary action (Section 10.0) is paused for staff until external investigation is complete.

Phase 3: Standard (Non-Illegal) Incidents

Step	Action	Decision Point
3.	**Record & Secure Evidence** Document the incident details, date, time, and content (URL/secure screenshot) on a designated investigation machine. Isolate the involved student/device.	**Is the incident a serious breach (e.g., severe cyber-bullying, bringing the school into disrepute, repeated unauthorized access)?**
4.	**Report Internally** Report the incident to the **Head of Department/Year** and the **Online Safety Officer (OSO)** via the school's reporting mechanism (e.g., Beacon Button/email).	**YES**

5.	**Initial Review & Decision (Involve Multiple Senior Staff)** Head of Dept/OSO consults with DSL/Headteacher to judge the substance and severity of the breach.	**Escalate to Headteacher/DSL** (Go to Step 6)
6.	**Headteacher/DSL Action** Determine the appropriate sanction (e.g., Suspension, Exclusion, Staff Disciplinary – Section 10.0). **Inform Parents/Carers.**	**Action Complete** (Go to Step 8)
7.	**Staff/Pupil Action** Issue a recorded **Warning/Minor Detention**. Implement technical action (e.g., temporary network access removal). **Inform Parents/Carers** where appropriate (Section 10.0).	
8.	**Close Incident Review** the school filtering/monitoring systems if the incident exposed a loophole. **Record** the incident, action, and outcome anonymously in the Online Safety Incident Log. **Monitor** the student/staff member.	