



KINGSDOWN SCHOOL

Online Safety Policy March 2026/27

Last reviewed on:	March 2026
Next review due by:	March 2027

1. Introduction and Scope
 2. Schedule for Monitoring and Review
 3. Roles and Responsibilities
 4. Education and Training
 5. Technical Safeguarding: Filtering, Monitoring, and Cyber-Security
 6. Artificial Intelligence (AI) Policy
 7. Reporting and Responding to Incidents
 8. Staff (and Volunteer) Acceptable Use Agreement (AUA)
 9. Educating Parents and Carers
 10. Role of the Online Safety Governor
 11. Appendix 1: Learner Acceptable Use Agreement
 12. Appendix 2: Parent/Carer Acceptable Use Agreement & Permission Forms
-

Kingsdown School Online Safety Policy (March 2026 Update)

1. Introduction and Scope

This policy outlines the commitment of **Kingsdown School** to safeguard members of the school community online in accordance with statutory guidance and best practice. **This policy applies to all members of the Kingsdown School community (including staff, learners, governors, volunteers, parents and carers, visitors, and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site where allowed.**

The school will manage online safety incidents through this policy and associated behaviour and anti-bullying policies. **Kingsdown School** maintains a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, and hatred.

2. Schedule for Monitoring and Review

- **Policy Development:** This policy was developed by the **Kingsdown School** Online Safety Group, led by **Karen Agambar**, the **Designated Safeguarding Lead (DSL)**, and **Lee Hathaway**, the **Online Safety Lead (OSL)**.
- **Meeting Frequency:** The Online Safety Group will meet **3 times per year** to oversee issues, monitor policy impact, and review filtering/monitoring logs.
- **Monitoring:** The **DSL** and **OSL** will monitor the implementation of this policy at regular intervals, at least once a year.
- **Approval and Reporting:** The Governing Body approved this policy and will receive a report on its implementation, including anonymised incident details, at least once a year.
- **Next Formal Review Date: March 2027.**

3. Roles and Responsibilities

The Headteacher and Senior Leaders The Headteacher has a duty of care for ensuring the safety of the school community and fostering a culture of safeguarding. Day-to-day responsibility is held by the **DSL**. Senior leaders ensure the **DSL**, **OSL**, and IT providers receive suitable training and work with the Governing Body to oversee filtering and monitoring systems.

Designated Safeguarding Lead (DSL) The **DSL** takes lead responsibility for safeguarding and child protection, including online safety, which is explicit in her job description. Responsibilities include:

- Understanding unique online risks, including those faced by learners with SEND.
- Meeting regularly with the Online Safety Governor to review anonymised incident logs and filtering reports.
- Receiving and managing reports of online safety incidents and deciding on referrals to external agencies.

Online Safety Lead (OSL) The **OSL** supports the **DSL** and is responsible for:

- Leading the Online Safety Group and promoting online safety education across the school.
- Liaising with curriculum leaders to ensure the online safety curriculum is planned, mapped, and evaluated.
- Identifying training and advice for staff, governors, and parents.

IT Provider IT staff have technical responsibility for maintaining filtering and monitoring systems, providing reports, and completing actions following system checks. They must ensure the school meets the **DfE Meeting Digital and Technology Standards**.

4. Education and Training

Learner Curriculum Kingsdown School provides a planned online safety curriculum (e.g., ProjectEVOLVE) for all year groups. Lessons are age-related, build on prior learning, and are threaded through PHSE, Literacy, and Computing. Learners are taught to:

- Be critically aware of content and validate accuracy (including AI-generated content).
- Respect copyright and intellectual property when using the internet and AI.
- Understand the importance of the Acceptable Use Agreement (AUA).

Staff and Governor Training

- **Staff:** All staff receive online safety training at induction, updated at least annually via meetings, e-bulletins, or INSET days.
- **Governors:** Governors participate in training to understand the school's filtering and monitoring provision and basic cyber-security standards.

5. Technical Safeguarding: Filtering, Monitoring, and Cyber-Security

Filtering and Monitoring The school implements appropriate systems to limit exposure to harmful content, in line with **DfE Filtering and Monitoring Standards**.

- **Filtering:** Illegal content is blocked using the Internet Watch Foundation (IWF) and Home Office terrorist content lists.
- **Monitoring:** The school monitors network use across all devices. The **DSL** urgently reviews and records the outcomes of all alerts.
- **Reviews and Checks:** Provision is reviewed at least annually by senior leaders, the **DSL**, and a governor. Technical checks are conducted at least termly to ensure the system is effective.

Cyber-Security (New January 2025) Kingsdown School follows the **DfE Cyber Security Standards** to prevent operational and financial impacts from cyber-attacks.

- **Risk Assessment:** The school conducts an annual cyber risk assessment, reviewed termly.
- **Backups:** Rigorous back-up routines include air-gapped copies off-site or in the cloud.
- **Access Control:** A documented access control model defines rights for all users; administrator passwords are kept in a secure location (e.g., school safe).

6. Artificial Intelligence (AI) Policy (Updated April 2026)

The school acknowledges the benefits of AI while mitigating risks through existing procedures.

- **Staff Use:** Staff must only use **school-approved AI services** and school-provided accounts for work purposes.
- **Data Protection:** Personal and sensitive data must be **anonymised** before being entered into AI tools.
- **Human Oversight:** AI should assist, not replace, human decision-making. All AI-generated content must be **fact-checked and reviewed** for accuracy and bias before sharing.
- **Reporting:** AI incidents, including data breaches or inappropriate outputs, must be reported immediately to the **DSL**.

7. Reporting and Responding to Incidents

Kingsdown School maintains clear reporting routes consistent with safeguarding, whistleblowing, and managing allegations policies.

- **Immediate Action:** Suspected illegal activity is escalated immediately to the Police or Local Authority.
- **Internal Response:** Non-illegal misuse is handled via the school's behaviour or disciplinary policies.
- **Staff Misuse:** Concerns regarding staff are reported to the Headteacher.

- **Record Keeping:** All incidents are logged (e.g., via the school MIS- Bromcom) to identify patterns and inform future updates to the policy or curriculum.

Kingsdown School Staff (and Volunteer) Acceptable Use Agreement

1. Introduction

Digital technologies are integral to the professional lives of all staff at **Kingsdown School**. These tools stimulate discussion, promote creativity, and enhance effective learning. While the school provides access to these systems to enhance your work, **Kingsdown School** has the right to protect its systems, and all users are entitled to safe access to the internet and digital technologies at all times.

2. Agreement Statement

I understand that I must use school systems in a responsible way to minimise the risk to the safety, privacy, or security of the **Kingsdown School** community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos, and values.

3. Professional and Personal Safety

- **Monitoring:** I understand that the school will monitor my use of school devices and digital technology systems.
- **Scope:** I understand that the rules set out in this agreement apply to the use of these devices and technologies both in and out of school, and to the transfer of personal or sensitive data (digital or paper-based).
- **Primary Purpose:** I understand that school devices are primarily intended for educational use and I will only use them for personal use within relevant school policies.
- **Account Security:** I will not disclose my username or password to anyone else, nor will I try to use any other person's credentials. I will store my passwords securely in line with the school's security policy.
- **Reporting:** I will immediately report any illegal, inappropriate, or harmful material or incidents I become aware of to the **Designated Safeguarding Lead (DSL)** or **Online Safety Lead (OSL)**.

4. Professional Communications and Conduct

- **Tone:** I will be professional in my communications and will not use aggressive or inappropriate language.
- **Files:** I will not access, copy, remove, or alter any other user's files without their express permission.
- **Images:** I will only take or publish images of others with their permission and in accordance with school policy. I will not use personal equipment to record these images unless I have explicit permission.
- **Official Systems:** I will only communicate with learners and parents/carers using official school systems sanctioned by the school. Such communication will always be professional in tone and manner.
- **Reputation:** I will not engage in any online activity that may compromise my professional responsibilities or the school's reputation.

5. Responsible Use of Artificial Intelligence (AI)

When using AI systems in my professional role at **Kingsdown School**, I will:

- Only use AI technologies approved by the school and school-provided accounts.
- Critically evaluate AI outputs for bias, discrimination, and accuracy before sharing or publishing.
- Ensure that I have explicit authorisation before uploading sensitive school-related information into AI systems and ensure all data is anonymised.
- Clearly label any documents, emails, or presentations influenced by AI to indicate AI assistance.
- Ensure that AI assists, but does not replace, human decision-making; final judgements affecting people must be made by a human.

6. Technical Security and Data Protection

- **Compliance:** I will abide by all relevant guidance and legislation, including **Keeping Children Safe in Education** and **UK GDPR**.
- **Filtering and Monitoring:** I will not access illegal or inappropriate content and will not attempt to bypass any filtering or security systems.
- **Personal Devices:** When using personal mobile devices in school, I will follow the same rules as if I were using school equipment.
- **Software:** I will not install unauthorised programmes or alter device settings on school equipment without consent from the **OSL** or IT provider.
- **Data Encryption:** I will only transport or share personal information as outlined in the Data Security Policy. Any digital personal data transferred outside the secure local network must be encrypted.
- **Maintenance:** I will immediately report any damage or faults involving equipment or software to the relevant technical staff.

7. Accountability and Sanctions

I understand that I am responsible for my actions both in and out of the school. I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This may include a warning, suspension, referral to the Governing Body, and, in the event of illegal activities, the involvement of the Police.

Staff/Volunteer Name: _____

Initial DSL: Karen Agambar

Initial OSL: Lee Hathaway

Signed: _____

Date: _____

Kingsdown School recognises that parents and carers play a crucial role in ensuring children use digital devices and services appropriately. Because many parents may have a limited understanding of online safety risks or underestimate how often children encounter harmful material, the school implements a variety of strategies to enhance their awareness and involvement.

Direct Engagement and Training

- **Workshops and Information Evenings:** The school provides regular opportunities for engagement through awareness workshops and parents' evenings. These sessions often focus on current issues, such as **Harmful Sexual Behaviour (HSB)** and the safe use of **Artificial Intelligence (AI)**.
- **Leadership Support:** **Karen Agambar**, the **Designated Safeguarding Lead (DSL)**, and **Lee Hathaway**, the **Online Safety Lead (OSL)**, are responsible for identifying and providing training and advice for parents and carers.
- **Learner-Led Education:** Learners are encouraged to pass on online safety messages they have learned in lessons to their families, and they may even lead sessions during school events to demonstrate safe practices.

Communication and Information Sharing

- **Policy Access:** The school's **Online Safety Policy** is published on the school website for all parents to review.
- **Regular Updates:** **Kingsdown School** uses newsletters, letters, the school website, and social media to share information about national and local online safety campaigns. This includes sharing "AI in our school" guides and newsletters specifically about HSB.
- **Incident Learning:** When online safety incidents occur, the school may share anonymous patterns or "lessons learned" with parents through regular briefings or newsletters to help them identify similar risks at home.

Guidance on Specific Risks

- **Acceptable Use Agreements (AUAs):** Parents are provided with copies of the learner AUAs to ensure they understand the school's expectations for responsible behavior.
- **Social Media and Digital Images:** The school publishes information about the appropriate use of social media and the risks associated with publishing digital images of children online. Parents are also urged to resolve concerns about the school privately rather than through public social media posts.
- **Reporting Routes:** The school website includes an online reporting process, making it easy for parents and the wider community to register concerns or report issues.

External Support and Resources

The school directs parents to expert external organisations for further guidance, including:

- **UK Safer Internet Centre (UKSIC)** and **Childnet** for general advice.
- **Internet Watch Foundation (IWF)** for reporting or removing inappropriate images.
- **Thinkuknow (NCA-CEOP)** for resources on staying safe online.
- **National Cyber Security Centre (NCSC)** for information on password security.

By providing these resources, **Kingsdown School** aims to empower parents to reinforce online safety messages at home and collaborate effectively with the school's safeguarding efforts

At **Kingsdown School**, a member of the governing body takes on the specific role of **Online Safety Governor** to provide strategic oversight and ensure the school meets its statutory safeguarding obligations. This individual acts as a bridge between the school's leadership and the board of governors, focusing on the following key areas:

Strategic Oversight and Monitoring

- **Policy Approval and Review:** The Online Safety Governor is responsible for the approval of the school's Online Safety Policy and for reviewing its effectiveness on a regular basis.
- **Meetings with Leadership:** They meet regularly with the **Designated Safeguarding Lead (DSL)** and the **Online Safety Lead (OSL)** to discuss current issues and monitor the progress of safety initiatives.
- **Reviewing Incident Reports:** They regularly receive and review collated, anonymised reports of online safety incidents. This data is used to inform future policy updates and identify emerging patterns.
- **Verification of Provision:** The governor checks that online safety education for learners and training for staff are taking place as intended.

Technical Safeguarding and Compliance

- **Filtering and Monitoring Oversight:** The Online Safety Governor ensures that the school's filtering and monitoring provision is reviewed and recorded at least annually.
- **System Checks:** They are involved in the annual review and periodic checks of the filtering and monitoring systems alongside senior leaders, the **DSL**, and IT service providers. This is particularly important when a new safeguarding risk is identified or when new technology is introduced.
- **Cyber-Security:** They are responsible for checking that the school meets DfE Cyber-Security Standards.

Leadership and Training

- **Online Safety Group Membership:** The Online Safety Governor is typically a member of the **Kingsdown School** Online Safety Group, which meets three times per year.
- **Specialised Training:** While all governors receive basic training to understand filtering, monitoring, and cyber-security, the Online Safety Governor receives a **higher level of training**. This includes basic cyber-security training and technical training to allow them to participate effectively in system reviews and checks.
- **Reporting to the Board:** They report on these findings and the overall implementation of the policy to the relevant governors' group or the full governing body.

Community Engagement

The Online Safety Governor supports the school in encouraging parents, carers, and the wider community to become actively engaged in online safety activities and awareness-raising

The following acceptable use agreements have been adapted for **Kingsdown School**, incorporating the leadership of **Karen Agambar** (DSL) and **Lee Hathaway** (OSL). These agreements are designed to ensure that all learners and parents/carers are responsible users who stay safe while using digital technologies.

Appendix A1: Learner Acceptable Use Agreement

I agree to use the school's digital systems responsibly to protect my safety, the security of the school systems, and others.

- **Personal Safety:** I understand the school will **monitor my use of its digital systems** and I will keep my usernames and passwords private. I will report harmful material or anything that worries me to a trusted adult.
- **Respecting Others' Work:** I will only use **AI tools approved by the school** and ensure my use is ethical and transparent. I will **fact-check and critically evaluate AI-generated content** for accuracy and bias before sharing.
- **Responsible Behaviour:** I will be polite and not bully or harass others. I will follow the age requirements for social media and protect the reputation of **Kingsdown School**.
- **Consequences:** I understand that failing to follow this agreement may lead to consequences, including **loss of access, detentions, or police involvement** in serious cases.

Signed student:

Appendix A4: Parent/Carer Acceptable Use Agreement & Permission Forms

Kingsdown School requests that parents sign the following to show their support in this important aspect of the school's work.

1. Digital Technologies Permission

As the parent/carers, I give permission for my child to have access to digital technologies at school. I understand that the school will take every reasonable precaution, including **monitoring and filtering systems**, to ensure learners are safe. I will encourage my child to adopt safe use at home and inform the school of any online safety concerns.

2. Use of Digital/Video Images

- **School Use:** I agree to the school taking digital/video images of my child to support learning and celebrate success in newsletters or on the website. The school will ensure children cannot be identified by their full names.
- **Parental Use:** I understand I am welcome to take images at school events for personal use, but **these must not be published on social networking sites** to respect the privacy of other learners.

3. Use of Cloud Systems

Kingsdown School uses cloud services to enable learners to collaboratively create, edit, and share files for school projects. I consent to my child having access to these services.

4. Use of Biometric Systems

The school uses biometric systems (e.g., for library or canteen access). No complete images of fingerprints are stored; they are converted into a secure string of numbers that cannot be reconstructed. I understand that I can withdraw consent at any time and that an alternative means of access will be provided if I do not consent.

Signed Parent/Carer:

At **Kingsdown School**, staff are encouraged to use AI tools to support their work, but they must adhere to strict rules regarding security, transparency, and professional accountability.

The specific rules for staff using AI include:

Approved Tools and Accounts

- **Official Services Only:** Staff must only use **AI services approved by the school** and must use **school-provided AI accounts** for all work purposes.
- **Prohibited Use:** Using AI services that have not been explicitly approved by the school is not allowed.

Data Protection and Privacy

- **Anonymisation:** Staff must ensure that any data input into AI tools is **anonymised** to avoid exposing personally identifiable or sensitive information.
- **Sensitive Information:** Internal documents, strategic plans, or sensitive data must not be entered into third-party AI tools unless they have been **explicitly vetted** for that purpose.
- **GDPR Compliance:** Staff must verify that any AI tool used for school-related work complies with **UK GDPR** and other relevant data protection regulations.

Human Oversight and Accuracy

- **Assistance, Not Replacement:** AI should assist, but **never replace**, human decision-making. Final judgments, particularly those affecting people (such as assessment or disciplinary matters), must always be made by a human.
- **Critical Evaluation:** All AI-generated content must be **fact-checked and critically evaluated** for accuracy, bias, and discrimination before being shared or published.

Transparency and Ethics

- **Clear Labelling:** Documents, presentations, or communications influenced by AI must include **clear labels or notes** indicating AI assistance to maintain transparency and build trust.
- **Intellectual Property:** Staff must respect copyright and intellectual property conventions. Care must be taken to ensure that learner work is not used to train generative AI models without appropriate consent.

Reporting and Discipline

- **Immediate Reporting:** Any AI-related incidents, including misuse, data breaches, or inappropriate outputs, must be reported immediately to the **Designated Safeguarding Lead (Karen Agambar)**.
- **Accountability:** Improper use of AI tools, including failures to adhere to data protection standards, is subject to **disciplinary action** as defined in the **Kingsdown School Staff Disciplinary Policy**

At **Kingsdown School**, staff are required to report any AI-related data breaches, misuse, or inappropriate outputs **immediately** to the **Designated Safeguarding Lead (DSL), Karen Agambar**.

The reporting process follows these established protocols:

- **Prompt Communication:** Staff must report incidents as soon as they are identified. **Quick reporting** is emphasised as it helps to **mitigate potential risks** and facilitates a prompt response.
- **Recording Incidents:** All AI-related incidents are recorded through the school's **normal recording systems**.

- **Urgency and Recognition:** Staff are expected to be trained to **recognise a possible breach** and understand the need for urgency in notifying the DSL.
- **Safeguarding Procedures:** Reporting must be in line with the school's wider **safeguarding procedures**.
- **External Referral:** Once a report is received, the **DSL** is responsible for managing the incident and deciding whether a referral to external agencies (such as the Police, ICO, or Local Authority) is necessary.

As noted in the **Kingsdown School** AI policy, any improper use of AI tools, including breaches of data protection standards or failure to report incidents, will be subject to **disciplinary action** as defined in the Staff Disciplinary Policy

Under the **Kingsdown School** Online Safety Policy (updated for March 2026), pupils are encouraged to take a proactive and responsible approach to reporting cyber-bullying. The school provides several clear reporting routes designed to be easily understood and followed by all members of the community.

Primary Reporting Mechanisms

- **Trusted Adults:** Pupils of all ages are instructed to report any online material or messages that make them feel worried, upset, or harassed to a **trusted adult** immediately.
- **Direct Reporting to Staff:** Learners should report suspected misuse or bullying to their teacher or the **Designated Safeguarding Lead (Karen Agambar)**, who holds lead responsibility for managing online safety incidents.
- **Online and Anonymous Tools:** The school maintains reporting systems that may include **online or anonymous reporting tools** (SHARPS) to allow pupils to register concerns confidently. Additionally, the school website does include an online reporting process.

Expectations for Pupil Conduct

- **Immediate Action:** Pupils are taught to report offensive, threatening, or bullying communications immediately and are strictly advised **not to respond** to such messages.
- **Reporting on Behalf of Others:** The curriculum teaches pupils the importance of reporting when they know someone else feels vulnerable or is being bullied online.
- **Zero-Tolerance Approach:** **Kingsdown School** operates with a zero-tolerance approach to incidents of online bullying, ensuring that all reports are dealt with as soon as practically possible.

Incident Management and Support

Once a report is made, the incident is managed through the Online Safety Policy in conjunction with the school's **Behaviour and Anti-Bullying policies**. The **Designated Safeguarding Lead** ensures all incidents are logged, typically within the school's Management Information System (Bromcom) to identify patterns and inform future educational programmes. The school also provides support strategies, such as peer support, for those affected by online bullying incidents.

As part of the 2026 policy schedule, these reporting procedures and their impact are reviewed by the **Online Safety Lead (Lee Hathaway)** and the Online Safety Group at least **three times per year**

At **Kingsdown School**, the handling of cyber risk assessments is a structured process integrated into the school's leadership and technical management. Based on the sources, the school follows these protocols:

Frequency and Oversight

- **Annual Assessment with Termly Reviews:** The school conducts a **formal cyber risk assessment annually**, which is then **reviewed every term**.
- **Risk Register:** Cyber security is explicitly included in the **Kingsdown School risk register** to ensure it receives high-level visibility.
- **Leadership Responsibility:** While the **Senior Leadership Team (SLT)** holds overall responsibility for technical security, they work in partnership with the school's **technology support partner** to identify and mitigate risks.

Scope of the Assessment

- **Critical Service Identification:** The assessment involves identifying the **most critical parts** of the school's digital and technology services and seeking formal assurance regarding their security.
- **System Audits:** There are regular **reviews and audits** of the safety and security of school technical systems to ensure they remain resilient against evolving threats.
- **AI Integration:** As part of the school's updated approach, the school **audits all AI systems** in use to assess their potential impact on school systems and procedures, maintaining an AI inventory that lists potential risks.

Role of Governors and Staff

- **Governor Verification:** The **Online Safety Governor** (and the wider Governing Body) receives at least **basic cyber-security training**. This enables them to verify that the school is meeting the **DfE Cyber-Security Standards**.
- **Staff Accountability:** All staff receive training on common cyber security threats. They are required to **report any suspicion or evidence of a security breach immediately** to the **Designated Safeguarding Lead (Karen Agambar)** or the **Online Safety Lead (Lee Hathaway)**.

Business Continuity and Resilience

- **Incident Management:** The findings of the cyber risk assessment inform the school's **business continuity and incident management plan**.
- **Technical Safeguards:** To support the risk assessment's goals, the school maintains **rigorous and verified back-up routines**, including copies stored off-site or in the cloud to protect against data loss during a cyber-attack.

As a reminder, the effectiveness of these procedures is monitored by the **DSL** and **OSL**, with the full policy scheduled for its next formal review in March **2027**

Under the updated **Kingsdown School** Online Safety Policy, the rules for students using mobile devices are governed by a focus on **educational purpose** and rigorous **technical safeguarding**.

Core Principles and Access

- **Educational Purpose:** The primary purpose of using any mobile device, whether school-owned or personally owned, in a school context is **educational**.
- **Permission Levels:** **Kingsdown School** determines which devices are permitted and their level of network access. While school-owned devices are generally allowed, the use of **personal mobile phones** during the school day is subject to specific restrictions by the Headteacher to reduce risks like distraction, bullying, and abuse.
- **Storage:** If personal devices are brought to school but not permitted in lessons, they must be kept in **appropriate, safe, and secure storage**.

Technical Safeguarding (Filtering and Monitoring)

- **Network Filtering:** All mobile devices connected to the school network—including those with 3G, 4G, or 5G capabilities, are subject to **filtering and monitoring** consistent with school policy.
- **Off-Site Protection:** School-provided devices have **school-based filtering applied regardless of their location**.
- **Bypassing Security:** Students are strictly prohibited from using proxy sites, VPNs, or other means to **subvert the school's filtering system**.

User Conduct and Responsibilities

- **Exams and Tests:** Mobile devices are **not permitted in tests or exams**.
- **Images and Video:** The **non-consensual taking or sharing of images/videos** of others is strictly forbidden. Students must only share respectful images of themselves or others when fully dressed.
- **AI and Accuracy:** When using mobile devices to access **Artificial Intelligence (AI)** services, students must **check the accuracy of content** and respect intellectual property.
- **Personal Responsibility:** Students are responsible for **charging and looking after their own devices**. **Kingsdown School** accepts no liability for the loss, theft, or damage of personal equipment.

Confiscation and Search Powers

- **Right to Search:** Authorised staff, under the direction of the **Designated Safeguarding Lead (Karen Agambar)**, have the right to **take, examine, and search** any device suspected of unauthorised or inappropriate use.
- **Examination of Data:** Staff may examine data or files on a confiscated device if there is a **"good reason"** (e.g., suspicion of an offence, risk of harm, or disruption of teaching).
- **Deletion of Material:** Authorised staff may **delete data or files** if their continued existence is likely to cause harm, provided the material is not suspected to be evidence of a criminal offence.

Cyber-Bullying and Reporting

- **Zero-Tolerance:** There is a **zero-tolerance approach** to using mobile devices for cyber-bullying, sexual harassment, or discrimination.
- **Reporting:** Students must immediately report any **offensive, threatening, or bullying communications** to a trusted adult and are advised not to respond to such messages.

The implementation of these rules is monitored by the **Online Safety Lead (Lee Hathaway)** and the Online Safety Group, which meets **three times per year**. The policy is scheduled for its next formal review on **March 2026**, with subsequent updates occurring annually every November

At **Kingsdown School**, the storage and management of air-gapped backups are governed by strict technical security standards designed to ensure resilience against cyber-attacks.

The specific storage rules for these backups include:

- **Network Separation:** Backups must be "air-gapped," meaning they are kept **network-separated** from the main school systems to prevent them from being compromised during a live cyber incident.

- **Location Requirements:** These air-gapped copies must be stored either **off-site** or securely **in the cloud**.
- **Rigorous Routines:** The school must maintain **rigorous and verified back-up routines** to ensure that data can be effectively restored if necessary.
- **Oversight:** While the **Senior Leadership Team** at **Kingsdown School** holds overall responsibility for technical security, they may delegate the daily management of these routines to identified roles, such as the IT provider. **Karen Agambar** (DSL) and **Lee Hathaway** (OSL) also monitor the implementation of these technical standards as part of the wider Online Safety Policy.
- **Verification:** The school's restoration plan must be tested to ensure it is effective in the event of a cyber-attack.

These protocols are a key component of the school's commitment to meeting the **DfE Cyber Security Standards**, which aim to protect against significant operational and financial impacts caused by unauthorised attempts to access or damage school data

If a staff member at **Kingsdown School** breaks the rules regarding Artificial Intelligence (AI), the response follows a structured process of reporting and disciplinary action as defined by the school's safeguarding and professional standards.

1. Immediate Reporting

Any suspected **AI misuse or data breach** involving a staff member must be reported immediately to **Karen Agambar**, the **Designated Safeguarding Lead (DSL)**. Following this initial notification, concerns regarding staff conduct are formally reported to the **Headteacher**.

2. Disciplinary Framework

The school treats the improper use of AI tools as a professional conduct issue. Responses are handled through the following channels:

- **Staff Disciplinary Policy:** Any failure to adhere to AI agreements—including breaching data protection standards or misusing sensitive information—is subject to disciplinary action as defined in the **Staff Disciplinary Policy**.
- **Normal Disciplinary Processes:** In all cases of AI misuse, the school will follow its **standard staff disciplinary processes**.

3. Potential Sanctions and Actions

The severity of the incident determines the specific response. According to the school's "Responding to Staff Actions" matrix and acceptable use templates, consequences may include:

- **Internal Referrals:** The matter may be referred to a line manager, the Headteacher, or HR.
- **Formal Warnings:** A staff member may be issued a formal warning.
- **Suspension:** For more serious breaches, the staff member may be suspended.
- **External Escalation:** In the event of illegal activities, the **Designated Safeguarding Lead** may refer the case to the Governors, the Local Authority/Trust, or the **Police**.

4. Specific AI Misuse Examples

Sanctions apply to a range of unacceptable AI-related behaviours, such as:

- **Data Protection Breaches:** Inputting sensitive school data or personally identifiable information into unvetted, third-party AI tools.
- **Copyright Infringement:** Using AI in a way that infringes on intellectual property or licensing regulations.
- **Lack of Oversight:** Failing to maintain human oversight or fact-check AI outputs, leading to the spread of misinformation.
- **Bypassing Security:** Attempting to use AI services to subvert the school's filtering or monitoring systems.

Note: The **Designated Safeguarding Lead** and the Headteacher are also responsible for ensuring that human oversight is maintained if AI tools are used to support the monitoring or reporting of such incidents, ensuring context and nuance are not missed.

Under the **Kingsdown School** Online Safety Policy updated for November 2026, pupils are provided with multiple, clear avenues to report cyber-bullying and other online concerns. The reporting process is designed to be easily accessible and is reinforced through the school's education programme.

Primary Reporting Routes

- **Trusted Adults and Staff:** Pupils are encouraged to report any online material or messages that make them feel worried, upset, or uncomfortable to a **trusted adult** immediately. This includes reporting directly to a teacher or to **Karen Agambar**, who serves as the **Designated Safeguarding Lead**.
- **Clear Procedures:** The school maintains **clear reporting routes** that are understood by all members of the community and are consistent with wider safeguarding and anti-bullying procedures.
- **Online and Anonymous Tools:** To ensure pupils feel confident in coming forward, **Kingsdown School** may provide **online or anonymous reporting systems**, such as SWGfL Whisper, or an online reporting process via the school website.

Instructions for Pupils

- **Do Not Respond:** Learners are specifically taught that if they receive a communication that is offensive, threatening, or bullying in nature, they must **immediately report it and must not respond** to the message.
- **Peer Reporting:** The policy encourages pupils to report not only their own concerns but also to speak up if they know someone else feels vulnerable or is being bullied online.
- **Evidence Preservation:** While pupils are advised not to engage with the bully, the **Designated Safeguarding Lead** is responsible for ensuring incidents are logged and recorded, which may involve saving evidence like URLs or screenshots for investigation.

Support and Education

- **Curriculum Integration:** Pupils are taught how to recognise cyber-bullying and how to use these reporting routes through a **planned, age-related online safety curriculum** (such as ProjectEVOLVE). This programme is overseen by the **Designated Safeguarding Lead** and **Lee Hathaway**, the Online Safety Lead.
- **Support Strategies:** **Kingsdown School** ensures that **support strategies**, such as **peer support**, are in place for those who are affected by or report online bullying.
- **Zero-Tolerance Culture:** The school operates with a **zero-tolerance approach** to cyber-bullying, ensuring that all reports are dealt with as soon as practically possible.

All incidents are logged by the **Designated Safeguarding Lead** to identify patterns, which helps the school improve its future preventative work and education programmes

Signed by :
Headteacher

Signed by :
Chair of Governors

Date :

Date :

Policy Last Updated: March 2026

Next Review Due: March 2027