



TEALBY PRIMARY SCHOOL

Aspire, Believe, Achieve

We want our pupils to move from us, confident, curious, articulate, creative, independent and well-prepared for their next stage. We want to produce collaborators, innovators, leaders and, more than anything else, young people who understand what it is to be human.

Online Safety Policy

September 2026

Aligned to Keeping Children Safe in Education 2026 and the LCC Safeguarding and Child Protection Policy 2026/27

Named Personnel with Responsibility for Safeguarding

Head Teacher: Zoe Humberstone

Chair of Governors: Rebecca Blackwood

Designated Safeguarding Lead (DSL): Zoe Humberstone

Deputy Designated Safeguarding Leads (DDSL): Chloe Brown & Christa Haslam

Safeguarding Governor: Rebecca Blackwood

Designated Teacher for Children in Care and Children Previously in Care: Zoe Humberstone

SEND/CO: Christa Haslam

Online Safety Coordinators: Christa Haslam/Zoe Humberstone

The Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL) have responsibility for ensuring that the safeguarding of children is central to the ethos of our school. They are suitably trained and experienced and carry out the duties of the DSL role as outlined in the most recent version of Keeping Children Safe in Education (KCSIE) and summarised in this policy.

This policy is reviewed annually, or sooner following national or local safeguarding changes to policy and procedure.

Next Review Date: September 2027

This version reflects: Keeping Children Safe in Education 2026 (in force from 1 September 2026) and the LCC Safeguarding and Child Protection Policy 2026/27.

Online Safety Policy

This policy should be read and understood in conjunction with the following documents:

- Keeping Children Safe in Education (KCSIE) 2026
- Searching, Screening and Confiscation (DfE)
- Mobile Phones in Schools (DfE) and Creating a Mobile Phone-Free Environment: School Case Studies (DfE)
- Generative Artificial Intelligence (AI) in Education, and Generative AI: Product Safety Expectations (DfE)
- Filtering and Monitoring Standards for Schools and Colleges (DfE) and Appropriate Filtering and Monitoring (UK Safer Internet Centre)
- Staff Code of Conduct
- Acceptable Use Agreements (staff, pupils and parents/carers)
- Behaviour Policy
- the LCC Safeguarding and Child Protection Policy 2026/27 and the school's Child-on-child Abuse Policy

This document has been developed by a working group made up of the Head Teacher, the Online Safety Coordinator, staff and governors, and is reviewed by that group on each renewal.

Scope of the Policy

This policy applies to all members of the school community – including staff, trainee teachers, pupils, volunteers, parents/carers, visitors and community users – who have access to and are users of the school's ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers the Head Teacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site, and empowers staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents of cyberbullying or other online safety incidents covered by this policy which take place outside school but are linked to membership of the school community. The Education Act 2011 extends these powers with regard to searching for, and the deletion of data from, electronic devices.

The school deals with such incidents within this policy and the associated Behaviour and Anti-bullying policies, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

In addition to the roles set out below, and to support this policy, the school maintains Acceptable Use Agreements, providing clear guidance on conduct, access to and use of the school system, removable media, downloading files, sharing information, social networks and devices, both school-owned and personal, in and out of school. Separate agreements exist for staff (forming part of the Staff Code of Conduct) and for parents/carers, who are asked to read and sign to acknowledge their

responsibilities, and to support the school in helping their children understand their own responsibilities.

School Governors

Governors are responsible for approving this policy and reviewing its effectiveness. The Full Governing Body receives termly information about online safety incidents and monitoring reports, and reviews online safety as part of its safeguarding monitoring procedures. In line with KCSIE 2026, governors also receive, at least annually, a written report on the outcome of the school's filtering and monitoring review, and satisfy themselves that appropriate systems remain in place.

Head Teacher and Senior Leaders

The Head Teacher has a duty of care for the safety, including the online safety, of members of the school community, though day-to-day responsibility for online safety is delegated to the Online Safety Coordinator. The Head Teacher is aware of the procedures to follow in the event of a serious online safety allegation being made against a member of staff, in line with the LCC Safeguarding and Child Protection Policy 2026/27 and KCSIE 2026 Part Four, and ensures the Online Safety Coordinator and other relevant staff receive suitable training to carry out their online safety roles and to train colleagues as needed. The Head Teacher holds regular meetings with the Online Safety Coordinator to review any incidents and agree on actions.

In line with KCSIE 2026, a named senior leader is responsible for ensuring the school's filtering and monitoring systems are reviewed for effectiveness at least once every academic year, working with the DSL and the school's IT support, with a record of checks kept covering all locations and devices, including school-owned devices used off-site.

Online Safety Coordinator

The Online Safety Coordinator takes part in SLT meetings and is responsible for:

- taking day-to-day responsibility for online safety policies and procedures;
- ensuring all staff are aware of the procedures to follow in the event of an online safety incident;
- liaising with the Local Authority as necessary;
- liaising with the school's technical support and external providers;
- receiving and logging online safety incidents to inform practice, policy review and development;
- meeting regularly with governors to discuss current issues, review incident logs and filtering procedures, and contribute to the annual filtering and monitoring review;
- attending relevant meetings and reporting regularly to the Head Teacher.

Network Manager / Technical Support

- ensures the school's technical infrastructure is secure and not open to misuse or malicious attack;
- ensures the school meets required online safety technical requirements and any relevant DfE/Local Authority guidance;

- ensures users may only access networks and devices through a properly enforced, regularly changed password policy;
- ensures the filtering policy is applied and updated regularly, and that its implementation is not the sole responsibility of any one person;
- keeps up to date with online safety technical information to carry out their role and to inform others;
- ensures use of the network, internet, learning platform, remote access and email is regularly monitored, so misuse or attempted misuse can be reported to the Head Teacher;
- ensures monitoring software systems are implemented and updated as agreed in the school's policies, and that appropriate filtering and monitoring systems are reviewed regularly for effectiveness, including in respect of AI-generated content and interactions with generative AI tools, while avoiding over-blocking that would unreasonably restrict what children can be taught.

Teaching and Support Staff

- maintain an up-to-date awareness of online safety matters and this policy;
- have read, understood and signed the Staff ICT Acceptable Use Agreement;
- report any suspected misuse or problem to the Online Safety Coordinator or Head Teacher;
- monitor the use of digital technologies, mobile devices and cameras in lessons and other activities, and implement current policies with regard to these devices, including the school's mobile phone-free expectations.

Designated Safeguarding Lead (DSL)

The DSL is trained in online safety issues and is aware of the potential for serious child protection and safeguarding issues to arise from: sharing of personal data; access to illegal and inappropriate material; inappropriate online contact with adults and strangers; potential or actual grooming; cyberbullying; and AI-generated or AI-altered imagery, including deepfakes and 'nudification' apps.

Pupils

- use the school's digital technology systems in accordance with the Home School Agreements;
- know and understand the school's rules on mobile devices and digital cameras, including the taking and use of images, and on cyberbullying;
- understand the importance of reporting abuse, misuse or access to inappropriate material, and know how to do so;
- understand the importance of good online safety practice when using digital technologies out of school, and that this policy covers their actions out of school where related to their membership of the school.

Parents/Carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet and mobile devices appropriately. The school helps parents/carers understand these issues through

parents' evenings, newsletters and letters, the school website and Learning Platform, and information about national and local online safety campaigns. Parents/carers are encouraged to support the school in promoting good online safety practice, and to follow guidance on the appropriate use of digital and video images taken at school events, access to parents' sections of the website/Learning Platform and online pupil records, and their children's personal devices in school, where and when this is allowed.

Education and Training

Staff and Volunteers

All staff receive online safety training as part of staff safeguarding training, including an understanding of their roles and responsibilities in relation to filtering and monitoring, in line with the DfE's Filtering and Monitoring Standards for Schools and Colleges and UK Safer Internet Centre guidance on Appropriate Filtering and Monitoring.

A planned programme of formal online safety training is made available to staff, regularly updated and reinforced; training needs are audited regularly and through performance management. All new staff receive online safety training as part of induction, ensuring they understand this policy and the Staff ICT Acceptable Use Agreement/Code of Conduct.

The Online Safety Coordinator receives regular updates through external training and by reviewing guidance released by relevant organisations. This policy and its updates are presented to and discussed by staff in staff/team meetings and/or INSET days as required, and the Online Safety Coordinator and DSL provide advice, guidance and training to individuals as needed.

Pupils

Regulation and technical solutions must be balanced by educating pupils to take a responsible approach; the education of pupils in online safety is an essential part of the school's online safety provision. Online safety is a focus across the curriculum and is reinforced by all staff.

The online safety curriculum is broad, relevant, provides progression, and includes opportunities for creative activities:

- a planned online safety curriculum is provided as part of Computing, PSHE and other lessons, regularly revisited, and reinforced through assemblies and pastoral activities;
- pupils are taught about online safety issues, including the risks of sharing personal details;
- pupils are taught, at an age-appropriate level, to be critically aware of the material and content they access online, to validate the accuracy of information, and to recognise misinformation, disinformation and conspiracy theories;
- pupils are taught to acknowledge sources and respect copyright when using material accessed online;
- pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and understanding how they can influence and participate in decision-making;

- pupils are helped to understand the need for the Pupil Acceptable Use Agreement, and encouraged to adopt safe and responsible use in and outside school, including safe and critical use of generative AI tools appropriate to their age;
- staff act as good role models in their use of digital technologies, the internet and mobile devices;
- where internet use is pre-planned, pupils are guided to sites checked as suitable for their use, with processes in place for dealing with unsuitable material found in searches;
- where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of websites visited;
- it is accepted that, for good educational reasons, pupils may occasionally need to research topics (for example racism, drugs or discrimination) that would normally be blocked; staff may request that filters be temporarily removed from those sites for the period of study, with any such request auditable and clearly reasoned.

Parents/Carers

Many parents/carers have only a limited understanding of online safety risks, yet play an essential role in educating and monitoring their children's online behaviour, and may underestimate how often children encounter potentially harmful material. The school provides information and awareness through curriculum activities, letters, newsletters, the website and Learning Platform, parents'/carers' information sessions, high-profile events and campaigns such as Safer Internet Day, and reference to trusted websites and publications such as saferinternet.org.uk and childnet.com/parents-and-carers.

The Wider Community

The school provides opportunities for local community groups and members of the community to benefit from its online safety knowledge and experience, including online safety messages targeted towards grandparents and other relatives, and online safety information for the wider community published on the school website.

Governors

Governors take part in online safety training and awareness sessions, particularly those on any subcommittee or group involved in technology, online safety, health and safety and safeguarding. This may include participation in school training and information sessions, attendance at assemblies and lessons, involvement in regular meetings and discussions, training through the National College, pupil voice activities, and receiving weekly updates in the school newsletter.

Technical Infrastructure, Filtering and Monitoring

Technical Infrastructure and Security

The school is responsible for ensuring its infrastructure and network are as safe and secure as reasonably possible, and that the policies and procedures approved within this policy are implemented. Where these services are provided by an external managed ICT provider, the school remains responsible for ensuring the provider fully complies with the school's policies, procedures and Acceptable Use Agreements, as well as any Local Authority and national guidance.

- The school's technical systems are managed to meet recommended technical requirements, with regular reviews and audits of safety and security.
- Servers, wireless systems and cabling are securely located, with physical access restricted.
- All users have clearly defined access rights to the school's technical systems and devices.
- Master/administrator passwords for the school ICT system are also available to the Head Teacher or another nominated senior leader, and kept securely.
- Education Lincs is responsible for ensuring software licence logs are accurate and up to date, with regular reconciliation of licences purchased against installations.
- Appropriate, regularly tested security measures protect servers, firewalls, routers, wireless systems, workstations and mobile devices from accidental or malicious threats; infrastructure and workstations are protected by up-to-date virus software.
- An agreed procedure is in place for temporary access for guests (for example trainee teachers, supply teachers and visitors) onto the school systems.
- **Cyber security is treated as a safeguarding priority, not solely an IT matter:** data security breaches can directly compromise pupil safety, and the school has regard to the Cyber Security Standards for Schools and Colleges when reviewing its systems, in line with KCSIE 2026.

Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective given the pace of change in web content, and levels of access and supervision vary according to pupils' age and experience. It is not possible to guarantee that unsuitable material will never appear on a school device.

- A log of all staff with unfiltered access to the internet is kept by Education Lincs.
- Internet access is filtered for all users. Illegal content, including child sexual abuse material, is filtered by the broadband/filtering provider using the Internet Watch Foundation CAIC list; content lists are regularly updated and internet use is logged and monitored.
- There is a clear process for requesting filtering changes, and filtering ensures children are protected from terrorist and extremist material.
- The school provides differentiated, user-level filtering, allowing different filtering levels for different groups of users (staff/pupils/visitors).
- **In line with KCSIE 2026, the effectiveness of the school's filtering and monitoring systems is formally reviewed at least once every academic year.** This review is led by the senior

leader responsible for filtering and monitoring, working with the DSL and IT support, covers all relevant locations and devices (including school-owned devices used off-site), and a written record of the review, and its outcome, is reported to governors.

- **Online risk categories reflect the DfE's 'four Cs' framework (content, contact, conduct and commerce), updated to include** exposure to disinformation, misinformation and conspiracy theories, and risks arising from interactions with generative AI tools or chatbots.
- School technical staff regularly monitor and record the activity of users on the school's technical systems, and users are made aware of this in the Staff ICT Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident and/or security breach.
- Pupils are made aware of the importance of filtering systems through the online safety curriculum, and of the consequences of attempting to subvert them.
- Staff are made aware of filtering systems through induction training, staff meetings, briefings and/or INSET.
- Parents are informed of the school's filtering policy through the Home School Agreement and online safety awareness sessions/newsletters.
- If staff or pupils discover unsuitable sites, the URL and content are reported to the internet service provider via the Online Safety Coordinator.
- Any material the school believes is illegal, or may place an individual at risk, is referred to the appropriate authorities: the Head Teacher, LADO, police and/or the Internet Watch Foundation.
- The use of computer systems without permission, or for inappropriate purposes, could constitute an offence under the Computer Misuse Act 1990.

Generative Artificial Intelligence (AI)

Generative AI tools are increasingly present in schools, both teacher-facing and pupil-facing, and bring benefits alongside new safeguarding, safety and legal considerations. In line with KCSIE 2026, the school understands and keeps under review the safety considerations and legal responsibilities relevant to any use of Generative AI, referring to the DfE's Generative Artificial Intelligence (AI) in Education guidance and Generative AI: Product Safety Expectations.

- Any AI tool used with pupils is risk-assessed and approved by the Senior Leadership Team before use, considering age-appropriateness, data protection, filtering/monitoring implications and the tool's terms and conditions.
- Staff and pupils are made aware that content generated or altered by AI, including images, video and text, can be inaccurate, biased or used to cause harm, including through deepfakes or other AI-generated or AI-altered intimate imagery, which is addressed further under Cyberbullying and Use of Digital and Video Images below.
- Filtering and monitoring arrangements are kept under review to reflect risks associated with generative AI, including unsupervised pupil interaction with AI chatbots and tools.

- Staff do not input personal or sensitive pupil data into public/consumer generative AI tools, in line with the school's Data Protection Policy.

Communication and Content

Website Content

The point of contact on the school website is the school address, school email and telephone number; staff or pupils' personal information is not published. The Head Teacher takes overall editorial responsibility and ensures content is accurate and appropriate. The website complies with the school's guidelines for publication, including respect for intellectual property rights, privacy and copyright. Where audio or video content is included (for example podcasts or video blogs), it does not allow children to be identified.

Learning Platforms

- All users require an appropriate password to access relevant content of the VLE, which must not be shared with others.
- SLT and staff regularly monitor pupil and staff usage, particularly message, communication and publishing tools.
- Pupils/staff are advised about acceptable conduct and use of the VLE.
- Only members of the current pupil, parent/carers and staff community have access to the VLE.
- All users are mindful of intellectual property and upload only appropriate content.
- When a user leaves the school, their account or access rights are disabled.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school-owned or personally owned, and might include smartphones, tablets, notebooks/laptops or other devices capable of using the school's wireless network and, through it, the wider internet, learning platform and cloud-based services.

In line with KCSIE 2026 and the DfE's Mobile Phones in Schools guidance, Tealby School operates a mobile phone-free environment by default. Pupils are not permitted to bring their own mobile devices, including mobile phones, into the classroom or to use them at any point during the school day, including lessons, time between lessons, breaktimes and lunchtime. Where a mobile phone is brought to school for a genuine reason, such as walking home independently, it must be handed in to the class teacher or the school office at the start of the day and collected once school has finished. Any exception to this default position is made only where reasonably necessary for an individual pupil's circumstances, for example a specific medical or additional need, and is agreed in advance with the Head Teacher.

Teaching about the safe and appropriate use of mobile technologies is integral to the school's online safety education programme, and is consistent with the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy and policies on theft or malicious damage. The school's Acceptable Use Agreements for staff, pupils and parents/carers give further guidance on the use of mobile technologies.

Use of Digital and Video Images

Digital imaging technologies bring significant benefits to learning, allowing staff and pupils instant use of images they have recorded or downloaded. However, staff, parents/carers and pupils need to

be aware of the risks associated with publishing digital images online: such images may provide avenues for cyberbullying, and digital images may remain available online indefinitely, potentially causing harm or embarrassment. The school informs and educates users about these risks and implements policies to reduce the likelihood of harm.

In accordance with Information Commissioner's Office guidance, parents/carers are welcome to take photographs and videos of their own children at school events for personal use. To respect everyone's privacy, these images should not be published or made publicly available on social networking sites, and parents/carers should not comment publicly on activities involving other pupils in any images.

Staff and volunteers may take digital/video images to support educational aims, but must follow school policy on the sharing, distribution and publication of those images; such images are taken only on school equipment, not staff members' personal devices. The school complies with data protection law, requests parental permission before taking images of pupils, and ensures published images do not identify pupils by name.

- Photographs published on the school website, or elsewhere, are carefully selected in line with good practice guidance.
- Care is taken that pupils in digital/video images are appropriately dressed, and not participating in activities that might bring individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Pupils' work is only published with the permission of the pupil and their parents/carers.

In line with KCSIE 2026, staff, pupils and parents/carers should be aware that images or videos of a sexual or intimate nature involving a child are treated with the same seriousness whether they are real, digitally altered, or wholly generated using AI (sometimes described as deepfakes or produced using 'nudification' apps), and that a safeguarding response is required whenever such content is made or shared, whether apparently consensual or non-consensual. Any concern of this nature is reported to the DSL immediately and managed in accordance with the school's Child-on-child Abuse Policy.

Communications

The official school email service is regarded as safe, secure and monitored; all users should be aware that email communications are monitored. Users must immediately report to the nominated person any communication that makes them feel uncomfortable, or that is offensive, discriminatory, threatening or bullying in nature, and must not respond to it. Any digital communication between staff and pupils or their parents/carers (email, social media, chat, blogs, the VLE, etc.) must be professional in tone and content.

Online Communication and Social Media

Staff

Staff should refer to the Staff Code of Conduct for detailed guidance on the use of online communications, and the Data Protection Policy regarding secure handling of data and communication between agencies.

Pupils

- Pupils may only use approved email accounts on the school system.
- Users are provided with a username and secure password by the Online Safety Coordinator, who keeps an up-to-date record of users and usernames; users are responsible for the security of their own credentials.
- Pupils are advised on security and privacy online, encouraged to set and regularly change passwords, deny access to unknown individuals, and block unwanted communications; and to approve and invite only known friends on social networking sites, keeping profiles private.
- Users are taught how to keep personal information safe online, including their real name, address, phone numbers, school, IM/email addresses, full names of friends/family, and specific interests or clubs.
- Users must not reveal personal details of themselves or others online, including tagging photos or video, or arrange to meet anyone they have met online.
- Pupils must immediately tell a responsible adult if they receive offensive emails.
- Pupils are expected to use email acceptably; sending images without consent, explicit images, or messages causing distress or harassment are significant breaches of the school's Acceptable Use Agreements and are dealt with accordingly.
- Emails sent to external organisations are written carefully and, where appropriate, authorised before sending, in the same way as a letter on school headed paper.

Staff wishing to use social media tools with pupils as part of the curriculum risk-assess the site before use, check its terms and conditions to ensure it is age-appropriate, and obtain documented consent from the Senior Leadership Team before using social media tools in the classroom. Personal publishing is taught via age-appropriate sites suitable for educational purposes, moderated by the school where possible. No member of the school community should publish specific and detailed private thoughts about the school, particularly anything that may be considered threatening, hurtful or defamatory. Concerns regarding pupils' use of social networking, social media or personal publishing sites, in or out of school, are raised with parents/carers, particularly where these concern pupils' underage use of a site.

Video Conferencing

Video conferencing (including Google Classroom, Zoom, FaceTime, Skype and similar tools) enables users to see and hear each other between different locations, with many potential educational benefits, and should take place using the school's wireless system where possible.

- Staff refer to the school's Remote Learning Policy and Agreement guidelines before children take part in video conferences.
- All video conferencing equipment in the classroom is switched off when not in use, and not set to auto-answer.
- Pupils ask permission from a teacher before making or answering a video conference call.
- Video conferencing is supervised at all times.

Emerging Technologies

Emerging technologies are examined for educational benefit, and a risk assessment is carried out before use in school is allowed.

Cyberbullying

Cyberbullying can be defined as the use of information and communication technology, particularly mobile phones and the internet, deliberately to hurt or upset someone. For most children, using the internet and mobile devices is a positive and creative part of everyday life; unfortunately, technology can also be used negatively. It is essential that pupils, staff and parents/carers understand how cyberbullying differs from other forms of bullying, how it can affect people, and how to respond to and address misuse. Cyberbullying, like all other forms of bullying, by or against any member of the school community, will not be tolerated.

Full details are set out in the school's Behaviour, Anti-bullying and Child-on-child Abuse policies, which include:

- clear procedures to investigate incidents or allegations of cyberbullying;
- clear procedures to support anyone in the school community affected by cyberbullying;
- recording of all reported incidents of cyberbullying;
- steps to identify the person responsible, where possible and appropriate, which may include examining school system logs, identifying and interviewing possible witnesses, and contacting the internet service provider and police if necessary.

Pupils, staff and parents/carers are expected to work with the school to support its approach to cyberbullying and its wider online safety ethos. Where an incident involves the making or sharing of a real or AI-generated/altered intimate image or video of a child, this is treated as a child protection matter under the school's Child-on-child Abuse Policy, in addition to any cyberbullying response.

Data Protection

Personal data is recorded, processed, transferred and made available in accordance with UK data protection law, comprising the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The school has ensured that:

- it has a Data Protection Policy;
- it has appointed a Data Protection Lead
- it holds the minimum personal data necessary to perform its functions, and does not hold it for longer than necessary for the purpose it was collected;
- data held is accurate and up to date, with inaccuracies corrected without unnecessary delay;
- the lawful basis for processing personal data (including, where relevant, consent) has been identified, documented, and set out in a Privacy Notice;

- where special category data is processed, a lawful basis and a separate condition for processing have been identified;
- Data Protection Impact Assessments (DPIAs) are carried out where required;
- there are clear, understood arrangements for access to, and the security, storage and transfer of, personal data, including adequate contractual clauses or safeguards where personal data is passed to third parties, such as cloud service providers, including any AI tools;
- procedures are in place to deal with individual rights, including Subject Access Requests;
- there are clear, understood data retention policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from an information risk incident, recognising the requirement to report relevant data breaches to the Information Commissioner's Office within 72 hours of the breach, where feasible;
- consideration has been given to the protection of personal data when accessed using remote access solutions;
- the school has a Freedom of Information Policy setting out how it will deal with FOI requests.

All staff receive data handling awareness/data protection training and are made aware of their responsibilities. Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure, password-protected computers and other devices, ensuring these are properly logged off at the end of any session;
- transfer data using encryption and secure, password-protected devices;
- where personal data is stored on a portable computer system, memory stick or other removable media, ensure the data and the device are encrypted and password-protected, that the device has approved virus and malware checking software, and that the data is securely deleted once transferred or no longer needed, in line with school policy.

Handling of Complaints

The school's Complaints Policy and procedures can be found on the school website, or a hard copy can be provided on request from the school office. Parents/carers and pupils are asked to work in partnership with the school to resolve issues.

Where complaints do not involve acts which are clearly illegal (for example, accessing child abuse images or distributing racist material), they are dealt with through the school's normal complaints procedures. Complaints regarding illegal activity are dealt with in line with the school's safeguarding and disciplinary procedures and, where required, involve contact with the police and could lead to criminal prosecution, as could clear cases of cyberbullying.

- Any complaint about staff misuse must be referred to the Head Teacher.

- Any complaint about the Head Teacher must be referred to the Chair of Governors.
- Where any member of the school community has breached the terms of their Acceptable Use Agreement, the school reserves the right to restrict their access to the school's internet.

Responding to Incidents of Misuse

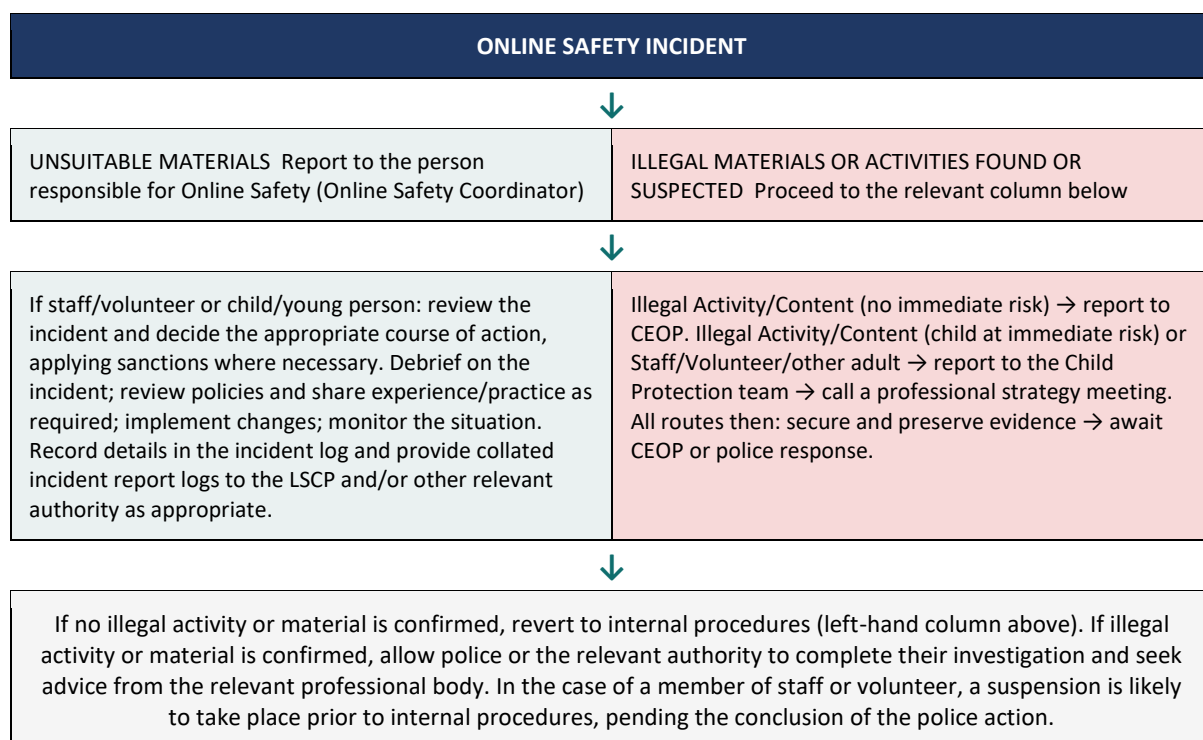
This guidance is for staff managing incidents involving the use of online services, and encourages a safe and secure approach to managing such incidents, which may involve illegal or inappropriate activity.

If there is any suspicion that a website may contain child abuse images, or of any other suspected illegal activity, refer to the right-hand side of the flowchart below and report immediately to the police.

It is expected that all members of the school community will be responsible users of digital technologies who understand and follow school policy. However, there may be times when infringements occur, through carelessness, irresponsibility or, very rarely, deliberate misuse. In the event of suspicion, all steps in this procedure are followed:

- more than one senior member of staff is involved in the process, to protect individuals if accusations are subsequently reported;
- the procedure is conducted using a designated computer not used by pupils, which can be taken off site by the police if needed, and the same computer is used throughout;
- relevant staff have appropriate internet access to conduct the procedure, with the sites and content visited closely monitored and recorded, to provide further protection;
- the URL of any site containing the alleged misuse is recorded, along with a description of the content causing concern; screenshots may also be recorded, printed, signed and attached to the incident form, except in the case of images of child sexual abuse;
- once fully investigated, the group judges whether the concern has substance and, if so, takes appropriate action, which may include internal disciplinary procedures, involvement of the Local Authority or a relevant national/local organisation, and/or police involvement;
- if content being reviewed includes images of child abuse, monitoring is halted immediately and referred to the police;
- other matters reported to the police include incidents of grooming behaviour, sending obscene material to a child, adult material potentially breaching the Obscene Publications Act, criminally racist material, promotion of terrorism or extremism, AI-generated child sexual abuse material, and other criminal conduct, activity or material;
- the computer in question is isolated as far as possible; any change to its state may hinder a later police investigation. These steps provide an evidence trail for the school and, potentially, the police, and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form is retained by the group for evidence and reference.

Flowchart: Responding to an Online Safety Incident



Policy Review

This policy is reviewed annually, or earlier if a change in legislation, statutory guidance or technological developments warrants it. In line with KCSIE 2026, the effectiveness of the school's filtering and monitoring systems is formally reviewed at least once every academic year, with the outcome reported to governors, in addition to this policy's own annual review cycle.