



Online Safety (E-Safeguarding) Policy

Reviewed: September 2026 • Next review: September 2027
(Online-safety and filtering/monitoring effectiveness review and risk assessment
completed at least annually; cyber-risk assessment reviewed termly)

Next review: September 2027

1. Introduction

Butler's Hill Infant and Nursery School fully recognises the contribution it can make to protect, and support, children in school and at home. The aim of this policy is to safeguard our pupils' and promote the safe use of internet and electronic communication technology on devices such as iPads, tablets, mobile phones and internet web browsers.

The internet and other technologies have an important role in the learning and teaching processes; however, we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies inside and outside of school.

This policy will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

This Online Safety (E-Safeguarding) Policy operates alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Computing Policy, Data Protection Policy, Acceptable Use Agreements and relevant curriculum policies. It should be read in the context of Keeping Children Safe in Education (KCSIE) 2026, Working Together to Safeguard Children, the EYFS statutory framework (where applicable), the Prevent duty, UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

Legal and guidance framework

This policy has been reviewed against: Keeping Children Safe in Education 2026 (in force from 1 September 2026); Working Together to Safeguard Children; the statutory Relationships Education, Relationships and Sex Education and Health Education guidance revised for September 2026; DfE Filtering and Monitoring Standards; DfE Cyber Security Standards for Schools and Colleges; DfE guidance on Generative Artificial Intelligence in Education and Generative AI Product Safety Expectations; UK GDPR; the Data Protection Act 2018; and the Data (Use and Access) Act 2025.

The school recognises online safety, information security and data protection as integral to safeguarding. Online safety is a running and interrelated theme across safeguarding, curriculum planning, staff training, the role of the DSL and deputies, filtering and monitoring, technology procurement and parental engagement.

Safeguarding

If a child comes across online content or contact that is distressing, upsetting, unsafe or suspicious, they should follow the school SMART code and tell a trusted adult immediately. Staff must respond in line with the Child Protection and Safeguarding Policy and report concerns promptly to the DSL or a deputy. Where a concern involves nude or semi-nude images, including AI-generated or digitally altered images, staff and

pupils must not intentionally view, copy, print, forward, save, screenshot or otherwise duplicate the imagery. The DSL will follow current UKCIS guidance on sharing nudes and semi-nudes and seek police/social care advice where required. For other online concerns, evidence should only be preserved where safe, lawful and necessary and should never involve creating or further sharing illegal or harmful content.

Telephone 0115 9525904 and ask to speak to the Designated Safeguarding Lead (Mrs Rachel Hallam) or the deputy safeguarding leads (Mrs Vicki Siddons, Mrs Emily Cunningham, Miss Chumun or Mrs Janet Radford).

email: head.teacher@butlershill.notts.sch.uk , vsiddons@butlershill.notts.sch.uk

If members of staff have Safeguarding concerns, these will be reported to the Designated Safeguarding Lead(s) following the school's Child Protection policy.

Teachers and adults in school have a Code of Conduct to follow.

Screening process in school

The school is covered by Netsweeper (via ATOM IT), a cloud-based web filter which covers all devices (Chromebooks, iPads, laptops and PCs) and provides unlimited data retention with 90 days of searchable data history. It is designed specifically for schools to help keep pupils safe. It provides remote monitoring and filtering, with both text and image-based alerts sent immediately to SLT/DSLs for them to review and action as needed.

The governing body retains strategic oversight of filtering and monitoring. The Headteacher/SIRO is the accountable senior leader, with operational oversight by the DSL and IT Lead and technical support from ATOM IT/Netsweeper. The school will review the effectiveness of filtering and monitoring at least once every academic year. The review will be led by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support, and will include recorded checks that filtering is working appropriately on all internet-connected devices in all relevant school locations. Findings, limitations, incidents, actions and any accepted risks will be reported to governors. The school will also consider pupils who may be at greater risk of harm, age/development, SEND and the need to avoid unreasonable over-blocking. Filtering and monitoring changes, exceptions and failures must be documented and escalated. Staff must know how to report a filtering or monitoring concern, including where harmful content is accessible, legitimate curriculum content is unreasonably blocked, alerts indicate safeguarding risk, or monitoring appears not to be operating as expected.

Any incidents that require further action are further recorded in our Safeguarding system.

Effective Practise in e-Safety

E-Safety depends on effective practise in each of the following areas:

- Education about responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safeguarding Policy;
- Secure, filtered broadband from the company Atom that uses 'Netsweeper (via ATOM IT)'
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used, including those associated with the PREVENT duty.

Writing and Reviewing the e-Safeguarding Policy

The e-Safeguarding Policy is part of the Subject Development Plan and relates to other policies including those for ICT, anti-bullying and for child protection

The school's named Online Safety Lead is Vicki Siddons. The Online Safety Lead works closely with the DSL, IT Lead, Headteacher/SIRO and technical provider.

- Our e-Safeguarding Policy has been written by the school. It has been agreed by staff and approved by governors.

2. Aims

- To set out the key principles expected of all members of the school community at Butler's Hill Infant and Nursery School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Butler's Hill Infant and Nursery School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

3. Scope of the Policy

- This policy applies to the whole school community including Butler's Hill Infant and Nursery School's Senior Leadership Team, school board of Governors

The governing body assigns overall accountability for filtering and monitoring to the Headteacher (SIRO) and operational oversight to the DSL and IT Lead. We complete an annual online-safety and filtering/monitoring risk assessment, review system effectiveness and limitations, and report outcomes to governors each autumn term. Governors also use the UKCIS 'Questions from the governing board' to support and challenge our approach., all staff employed directly or indirectly by the school, volunteers and all pupils.

- Butler's Hill Infant and Nursery School's Senior Leadership Team and school board of Governors

The governing body assigns overall accountability for filtering and monitoring to the Headteacher (SIRO) and operational oversight to the DSL and IT Lead. We complete an annual online-safety and filtering/monitoring risk assessment, review system effectiveness and limitations, and report outcomes to governors each autumn term. Governors also use the UKCIS 'Questions from the governing board' to support and challenge our approach. will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.

- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other e-Safeguarding related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy and the anti-bullying policy and will, where known, inform parents and carers of incidents of inappropriate e-Safeguarding behaviour that takes place out of school.

4. Review and Ownership

- The school has appointed an e-Safeguarding leader (Vicki Siddons) who will be responsible for document ownership, review and updates.

- The e-Safeguarding policy has been written by the school e-Safeguarding leader, alongside the Senior Leadership Team, and is current and appropriate for its intended audience and purpose.
- The e-Safeguarding policy is reflected in many other school policies such as the computing policy, Child Protection policy, Whistleblowing policy and Anti-bullying policy.
- The school e-Safeguarding policy has been agreed by the Senior Leadership Team and approved by governors.
- This policy will be reviewed at least annually and sooner following significant changes to technology, systems, guidance, legislation, safeguarding risks or a serious online/cyber incident. The school will also carry out an annual review of its overall online-safety approach, supported by a risk assessment reflecting the risks faced by its pupils.
- All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

5. Communication of the Policy

- Our Senior Leadership Team and class teachers will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.
- The e-Safeguarding policy will be provided to and discussed with all members of staff and reviewed annually.
- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used.

6. Roles and Responsibilities

We believe that e-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community will contribute:

•

The Senior Leadership Team

- The Headteacher, supported by the designated e-Safeguarding lead, is ultimately responsible for e-Safeguarding provision including safeguarding for all members of the school community.

The Headteacher/SIRO and SLT digital lead will ensure cyber risk is assessed annually and revisited at least termly, and that cyber-security responsibilities, incident response, business continuity and data-breach arrangements are understood.

The SLT member responsible for filtering and monitoring will lead the annual effectiveness review, supported by the DSL and IT support, ensure recorded checks are completed across all internet-connected devices/locations and ensure concerns are escalated and actions tracked.

- The Headteacher and Senior Leadership Team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.

Responsibilities of the e-Safeguarding Leader

- To promote an awareness and commitment to e-Safeguarding throughout the school
- To be the first point of contact in school on all e-Safeguarding matters
- To take day-to-day responsibility for e-Safeguarding within school and to have a leading role in establishing and reviewing the school e-Safeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated Safeguarding Governor
- To create and maintain e-Safeguarding policies and procedures
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that e-Safeguarding education is embedded across the curriculum
- To recognise the additional online risks that some children may face, including pupils with SEND or other vulnerabilities, and ensure teaching, supervision and support are appropriately adapted.
- To ensure the curriculum reflects the four areas of online risk (content, contact, conduct and commerce), including age-appropriate teaching about misinformation/disinformation, harmful online challenges, scams, online sexual harm, AI-generated/deepfake content and safe use of generative AI.
- To ensure that e-Safeguarding is promoted to parents and carers
- To liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safeguarding incident
- To ensure that an e-Safeguarding incident is recorded on COMPASS.
- To ensure that the school Acceptable Use policies are current and pertinent.

Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the e-Safeguarding Leader
- To develop and maintain an awareness of current e-Safeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To understand that filtering and monitoring do not replace professional supervision, curiosity or safeguarding judgement, and to report concerns or system failures immediately through school procedures.
- To use only school-approved digital and generative-AI tools for school business; never enter personal, special-category, safeguarding or confidential school information into an unapproved AI system; and check AI outputs for accuracy, bias, suitability and safeguarding risk before use.
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed e-Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of ICT technician/technical staff

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safeguarding related issues that come to your attention to the eSafeguarding Leader.
- To develop and maintain an awareness of current e-Safeguarding issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times

- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted

Responsibilities of pupils

- To know and understand school policies regarding cyber bullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to - using the SMART rules
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To understand, in an age-appropriate way, that images, videos, messages and voices can be altered or generated using AI and may be false, harmful or used to trick people; pupils should not create or share harmful, humiliating or sexualised AI-generated content and should tell a trusted adult if worried.

Responsibilities of parents and carers

- To help and support the school in promoting e-Safeguarding

To read, understand and promote the school pupil Acceptable Use Policy with their children

- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To engage with school information about online safety, including the school's filtering and monitoring arrangements, age-appropriate use of devices and apps, generative AI, scams, misinformation, harmful content and reporting routes.
- To agree to and sign the school's permissions form which clearly sets out the use of photographic and video images outside of school
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. This message is reinforced at the start of all public events.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written instruction if they do NOT wish for any images of their child to be used.

Responsibilities of the Governing body

- To read, understand, contribute to and help promote the school's e-Safeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To oversee cyber-security risk as part of safeguarding and strategic risk management, including assurance around annual cyber-risk assessment, termly review, access controls, backups, incident response and staff awareness.
- To ensure appropriate filtering and monitoring systems are in place; receive assurance that their effectiveness is reviewed at least annually; understand significant risks, limitations, incidents and actions; and use UKCIS governing-board questions or equivalent challenge tools.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school

- To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school
- To ensure appropriate funding and resources are available for the school to implement its e-Safeguarding strategy

Responsibilities of the Child Protection Designated Person

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate online contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyber bullying and the use of social media for this purpose

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to esafeguarding and the safe use of technologies
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school

7. Managing Digital Content

Using images, video and sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published.
 1. On the school website
 2. In the school prospectus and other printed promotional material, e.g. newsletters
 3. In display material that may be used around the school
 4. In display material that may be used off site
 5. Recorded or transmitted on a video or via webcam in an educational conference

This will be done via the permissions form included in the welcome pack for new starters.

- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.

- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network or school owned cloud storage and never transferred to personally-owned equipment.
- Images, video and audio will be retained only for as long as there is a clear, documented purpose and in line with the school's retention schedule, privacy information and data-protection requirements. Images of former pupils will not be retained indefinitely merely for possible future promotional use.
- AI-generated or digitally altered images of pupils must not be created or published unless there is a clearly defined educational purpose, an approved tool and appropriate safeguarding/data-protection assessment. Sexualised, humiliating or deceptive deepfake content involving children is prohibited and will be treated as a safeguarding concern.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- All staff have the responsibility of deleting the images when they are no longer required.

8. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- Teaching will address the four areas of online risk identified in KCSIE 2026: content, contact, conduct and commerce. This includes age-appropriate learning about harmful and illegal content, online contact and grooming, bullying and image-sharing, scams/phishing and inappropriate advertising, misinformation/disinformation, deepfakes and safe/critical use of generative AI.
- We will provide a series of specific e-Safeguarding-related lessons in specific year groups as part of the Computing curriculum / PSHE curriculum.
- We will celebrate and promote e-Safeguarding through whole-school activities, including assemblies and the promotion of Safer Internet Day.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying.

- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse icon.

All staff receive safeguarding and child protection training at induction, including online safety and an understanding of the expectations, applicable roles and responsibilities for filtering and monitoring. Training is regularly updated and all staff receive safeguarding and online-safety updates as required and at least annually. From September 2026, training and updates will include relevant emerging risks such as generative AI, AI-generated/deepfake imagery, online sexual harm, scams/phishing, misinformation/disinformation and the reporting/escalation of filtering or monitoring failures.

- Our staff receive regular information and training on e-Safeguarding issues in the form of annual updates, staff meetings etc.
- As part of the induction process all new staff receive information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safeguarding activities and awareness within their curriculum areas.

9. Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

The school will work towards and, where the DfE standard specifies current expectations, implement the DfE Cyber Security Standards for Schools and Colleges, including secure accounts and access, supported/up-to-date systems, anti-malware/firewall controls, backups, cyber-awareness training and incident reporting.

New digital services, apps, cloud platforms and AI-enabled products will be subject to proportionate safeguarding, privacy, security and procurement checks before approval. Where processing is likely to result in high risk to individuals, the school will complete a Data Protection Impact Assessment (DPIA) with advice from the DPO.

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Pupils will access the internet using year group logins, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

10. Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or a school's or local authority's network being infected or attacked. The school has a responsibility to ensure that all elements of the school infrastructure and network equipment are as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets should be controlled through the use of appropriate username and password complexity policies.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
 - Multi-factor authentication (MFA) must be enabled for staff accounts with access to cloud services or remote access to on-site systems, and for IT administrative accounts, in line with the DfE cyber-security core standard. Where MFA is unavailable, compensating controls and stronger authentication will be applied.
- Pupils will have a generic year group logon to all school ICT equipment.

- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords. Staff are reminded that they:
 1. Do not write down system passwords.
 2. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
 3. Always use your own personal passwords to access computer based services, never share these with other users.
 4. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
 5. Never save system-based usernames and passwords within an internet browser.

All access to school information assets will be controlled via username and password.

- No user should be able to access another user's files unless delegated permission has been granted.
 - Access to personal data is securely controlled in line with the school's personal data policy.
 - The school maintains a log of all accesses by users and of their activities while using the system.
 - Users should create different passwords for different accounts and applications.
 - Password strength will be enforced at system level using current NCSC/DfE guidance (for example, machine-generated passwords or three random words). Passwords must be unique to the user and changed immediately where compromise is suspected. The school may use approved password managers and single sign-on solutions where these improve security and are appropriately managed.
- % * () - + = , < > : : " ') : the more randomly they are placed, the more secure they are.

11. Emerging Technologies

Digital technology develops rapidly and may create both educational opportunities and new safeguarding, privacy, security and ethical risks. The school will consider emerging technologies, including generative AI, through a child-centred safeguarding and risk-management approach before use.

Generative Artificial Intelligence (AI)

Staff must not enter personal data, special-category data, safeguarding records, confidential material or identifiable pupil work into unapproved public AI tools.

Where an AI system processes personal data, the school will establish a lawful basis, provide appropriate transparency information and complete a DPIA where required. AI-generated outputs must be checked by a competent adult before being relied upon or shared.

Any staff-facing or pupil-facing generative-AI use must be approved for the intended purpose and considered against DfE guidance and product-safety expectations. Risk assessment will consider safeguarding, age appropriateness, filtering/monitoring, accuracy and bias, intellectual property, security and data protection. Pupils will use AI only where age-appropriate, educationally justified and suitably supervised.

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safeguarding point of view. We will regularly amend the e-Safeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-Safeguarding risk.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- Emerging technologies can incorporate software and/or hardware products.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the e-Safeguarding policy is adequate and that the implementation of the e-Safeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

12. Filtering Internet Access

Filtering is preventative and monitoring helps identify potentially concerning online activity. In line with KCSIE 2026 and the DfE Filtering and Monitoring Standards, the school will use appropriate filtering and monitoring to limit exposure to illegal, inappropriate and harmful content while avoiding unreasonable restrictions on teaching and learning. Filtering and monitoring are part of, not a substitute for, effective supervision, education and safeguarding practice.

- The school uses a filtered internet service. The filtering system is provided by Netsweeper (via ATOM IT).
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-Safeguarding Leader. All incidents should be documented.
- The effectiveness of filtering and monitoring will be reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support. The review will include recorded tests on all internet-connected devices in all relevant locations, consideration of pupil age and vulnerability, emerging risks (including generative AI), over-blocking, alert handling, escalation routes and service-provider performance.

•
Pupils will use age-appropriate tools to research internet content.

- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

13. Internet Access Authorisations

Schools should allow internet access to staff and pupils on the grounds that it is required for either work-related purposes or for educational need. The school should keep a record of who has access to the internet and what internet filtering policy will be applied to the individual user. By documenting access requests and authorisations a school has a full audit trail of when and to whom access has been granted.

- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.

14. Email

Electronic mail (email) is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place.

-
- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
(unless granted permission from the Headteacher)
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

14.1. Email usage

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Confidential and personal information must be shared only where necessary and by an approved secure method proportionate to the risk. Staff must follow the school's data-protection and information-sharing procedures and seek advice from the DPO/DSL where unsure.
- Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.

-
- Chain messages will not generally be permitted (please check with the Headteacher) or forwarded on to other school-owned email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations or parents, are advised to carbon copy (cc) or include the Headteacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence.

15. Using Blogs, Wikis, Podcasts, Social Networking and Other

Ways for Pupils to Publish Content Online

If we use blogs and other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within secure areas on the school website or Class Dojo app.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the school website and postings should be approved by the Headteacher before publishing. Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

•
16. Mobile Phone Usage in School

General issues

- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time.
- Mobile phones and personally owned mobile devices brought in to school by staff are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Teachers are to use school mobile phones (non smart, non camera phones) when on school trips.

Pupils' use of personal devices

- If a pupil brings a mobile phone into school the device will be handed to the class teacher at the start of the day and returned at the end of the day. If a pupil breaches this, the phone will be confiscated and held in a secure place. Mobile phones will be released back to parent(s) / Carer(s).

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- Staff are not permitted to use their mobile phones in school when there are children present.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose (unless otherwise agreed by the headteacher).
- If a member of staff breaches the school policy then disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then they should use the school mobile phones.

•
Senior Information Risk Owner (SIRO) - Headteacher

The Senior Information Risk Owner is a senior member of staff (normally the headteacher) who is familiar with information risks and the organisation's response.

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management
- 17.2 Information Asset Owner (IAO) - School and Finance Officer

The role of the IAO is to understand:

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed off

Although Butler's Hill Infant and Nursery School has appointed these key roles, the handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

The school community will carry out its duty of care for information assets in line with UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together referred to in KCSIE 2026 as data protection laws.

- Personal data will be collected, recorded, used, shared, retained and disposed of lawfully, fairly, transparently and securely in accordance with UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, and the school will be able to demonstrate compliance.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl+Alt+Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.

-
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email or post) are appropriately secured.
All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

18. Management of Assets

At Butler's Hill Infant and Nursery School we have software and hardware assets for both educational and administrative purposes. All equipment and software comes at a cost to the school and is therefore controlled and documented appropriately.

By maintaining valid inventories, Butler's Hill Infant and Nursery School is in a position to extract full value from our purchases as educational activities can be based and planned around the assets we hold. It should also not be overlooked that recording information on all equipment can also assist in hardware replacement programmes and software upgrades, as spending can be planned against asset age and specification.

The school is aware that any old hardware such as laptops, PCs, servers and removable media needs to be formatted prior to disposal (or through a third party) to ensure no sensitive or personal data remains on old hardware.

- Details of all school owned hardware will be recorded in a hardware inventory.
- Details of all school owned software/licences will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will be securely erased or physically destroyed using an appropriate, verifiable method before disposal or reuse. Where a third party is used, the school will obtain suitable

- assurance/certification of secure data destruction and comply with data-protection and environmental requirements.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2018

Remote Education and Online Learning

Where remote education is required, the school will follow current DfE safeguarding and remote-education guidance. Platforms and accounts will use appropriate security, access controls and moderation. Safeguarding expectations, reporting routes, data protection, staff conduct and online-safety arrangements apply equally to remote learning.

These remote learning platforms are safeguarded by individual pupil passwords and link directly to the class teacher (no third parties have access or share information). Passwords should not be shared with anyone outside your household. Teachers regularly monitor these platforms to mark and comment on pupil work. Uploading content and commenting on work is controlled by the class teacher. Content should be strictly school based and these online platforms should not be used to communicate or share content with other pupils. Any inappropriate text, audio recordings, videos or photos will be reviewed by the school designated safeguarding leaders and the appropriate action taken.

Live lessons will take place and will be accessed through Microsoft Teams, children will receive an invite for these lessons.

Code of conduct for remote learning and live lessons

- Online work should be undertaken in a shared space in the home environment
- Parents/carers will be given age-appropriate online-safety guidance for home use, including supervision, device/app settings, parental controls and reporting routes. The school will avoid endorsing specific commercial products unless these have been formally assessed and the recommendation is kept under review.
- Children should be dressed appropriately for the lesson
- Children should be 'ready to learn' and follow the school's Respect behaviour rules
- Any child who disrupts the lesson may be removed and their behaviour addressed at a later time by the class teacher
- All teaching will be recorded and these recordings can be viewed by the HT and Safeguarding leads.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

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

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

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

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Date:

Appendix 3: online safety training needs – self audit for staff

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

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Filtering & Monitoring Accountability Roles

Role	Named Person / Responsibility
Accountable Owner	Headteacher (SIRO) - overall accountability
Operational Leads	DSL & IT Lead - daily oversight and escalation
Technical Administration	Netsweeper (via ATOM IT) - provides filtering & monitoring service, reports to IT Lead
Governors	Receive annual online-safety risk assessment and termly updates

Executive Summary - Online Safety Policy (KCSIE 2026 Alignment)

This executive summary highlights the September 2026 revisions made following review against KCSIE 2026 and current DfE online-safety, filtering/monitoring, cyber-security, generative-AI and data-protection guidance. Policy compliance must be supported by effective implementation, evidence of reviews/checks, staff training and governor oversight.

Key Updates:

- Staff training: induction and regular safeguarding training include online safety and filtering/monitoring responsibilities; updates are provided as required and at least annually, including emerging AI/deepfake and online-harm risks.

Filtering & monitoring: effectiveness is reviewed at least once every academic year by the responsible SLT member with DSL and IT support; checks cover all internet-connected devices and relevant locations and are recorded. Governors receive assurance, risks and actions.

Whole-school approach: online safety is an interrelated safeguarding theme across policies, curriculum, staff training, parental engagement, DSL work and technology use, structured around content, contact, conduct and commerce.

Governance: governors receive annual online-safety/filtering-monitoring assurance, challenge using UKCIS questions or equivalent, and oversee cyber risk as part of safeguarding and strategic risk management.

- Incident management: All online-safety incidents logged on COMPASS and feed into the annual risk assessment.

- Updated resources: Useful links refreshed to include CEOP Education, CSA Centre, The Children's Society, Lucy Faithfull Foundation, and Education for a Connected World framework.

2026 legal/guidance update: references now include KCSIE 2026, revised RSHE guidance, DfE Filtering and Monitoring Standards, DfE Cyber Security Standards, generative-AI guidance/product-safety expectations, UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025.

This summary should be read alongside the full policy. It enables leaders, staff, and governors to quickly see how statutory requirements are met and what mechanisms ensure annual review and accountability.

Appendix 4: Additional Acceptable Use Requirements – September 2026

- Personal data must be shared only when necessary, with authorised recipients and through approved secure systems; data-protection incidents must be reported immediately in accordance with school procedures.
- Staff accounts with access to cloud services/remote systems and IT administrative accounts will use MFA in line with DfE cyber-security requirements.
- Users must report phishing, scams, suspicious links/messages, unexpected MFA prompts, compromised passwords or suspected cyber incidents without delay.
- Pupils must not use AI or digital tools to create, alter or share harmful, humiliating, deceptive or sexualised images/audio/video of any person. Concerns must be reported to a trusted adult immediately.
- Staff must use only school-approved generative-AI systems for school business and must not enter confidential, safeguarding, personal or special-category data into unapproved AI services.

-
- Users must not attempt to bypass, disable or interfere with filtering, monitoring, security controls or device-management settings, and must report suspected failures promptly.

These requirements supplement the existing pupil/parent and staff/governor/volunteer/visitor Acceptable Use Agreements. They apply to all users of school systems and school-related digital services.

September 2026 Review Record

Review basis: Keeping Children Safe in Education 2026; DfE Filtering and Monitoring: core standard (updated August 2026); DfE Cyber Security: core standard (updated August 2026); DfE Data Protection in Schools guidance (updated July 2026); UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; and associated DfE/UKCIS online-safety and generative-AI guidance. All September 2026 amendments/additions in this document are highlighted yellow for governor/staff review.