



## **Context**

### **September 2026 statutory and safeguarding update**

This policy is written in line with Keeping Children Safe in Education 2026 (KCSIE), Teaching Online Safety in Schools, the revised statutory Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance in force from 1 September 2026, the DfE filtering and monitoring standards, the Online Safety Act 2023, and current data protection and cyber-security requirements.

The internet and digital technology are widely used in school by staff and pupils. KCSIE 2026 makes clear that safeguarding applies online as well as offline and that technology is a significant component in many safeguarding and wellbeing issues. It is the responsibility of all staff to help ensure pupils use technology safely and responsibly in school and develop the knowledge and confidence to stay safe beyond school.

## **What are the current main online safety risks**

Online safety risks are categorised as the 4 Cs: Content, Contact, Conduct and Commerce. In line with KCSIE 2026, these include:

- Content: illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact: harmful online interaction with other users or generative AI applications that simulate interaction, including peer pressure, commercial advertising, grooming and exploitation for sexual, criminal, financial or other purposes.
- Conduct: online behaviour that increases the likelihood of, or causes, harm, including online bullying and the making, sending or receiving of explicit images, including images generated using AI.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and financial scams.

These categories overlap and should inform safeguarding, curriculum, staff training, parental engagement and the school's filtering and monitoring arrangements.

## **Scope of the policy**

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both inside and outside of school.

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 cyberbullying, or other online safety incidents covered by this policy, which may take place outside of Butler's Hill Infant and Nursery School.

The school will deal with such incidents within this policy (and the associated E-Safeguarding, Cyber Awareness, 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.

## **Aim of the policy**

Butler's Hill Infant and Nursery School embraces positive impact and educational benefits that can be achieved through appropriate use of the internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and children to unacceptable risks and dangers. We aim to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

It is equally important that staff have access to regular Online Safety training and are informed of any current thinking or changes in practice. We also have a duty of care to our parents/carers and offer Online Safety updates via newsletters and information on the school website and Class Dojo.

### **Legislation and Guidance**

This policy is based on the Department for Education's statutory safeguarding guidance Keeping Children Safe in Education 2026 and should be read alongside the school's Child Protection/Safeguarding, Behaviour, Staff Code of Conduct, Data Protection, Mobile Phone and related policies. It also has regard to:

#### **Teaching online safety in schools**

#### **Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff**

Relationships Education, Relationships and Sex Education (RSE) and Health Education: statutory guidance (revised guidance in force from 1 September 2026)

#### **Searching, screening and confiscation**

DfE Filtering and Monitoring: core standard (updated 25 August 2026)

DfE Cyber Security: core standard (updated in 2026, including Cyber Essentials 2026 requirements)

Generative AI in education and Generative AI: product safety standards (updated January 2026)

DfE Data protection in schools guidance, including the Data (Use and Access) Act 2025 changes in force from 8 July 2026

Online Safety Act 2023 and Ofcom child-safety duties relevant to regulated online services

Prevent duty guidance and the school's Prevent risk assessment

Mobile phones in schools guidance and KCSIE 2026 expectations for a mobile phone-free school environment by default

It reflects relevant legislation including the Education Act 1996 (as amended), Education and Inspections Act 2006, Equality Act 2010, Education Act 2011, Children and Social Work Act 2017, Data Protection Act 2018, UK GDPR, Data (Use and Access) Act 2025, Online Safety Act 2023 and other safeguarding legislation applicable to schools. The school will keep this policy under review when statutory requirements or DfE standards change.

The policy also takes into account the National Curriculum computing programmes of study.

### **Roles and responsibilities**

#### **The Designated Safeguarding Lead(s):**

KCSIE 2026 makes clear that the designated safeguarding lead has lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL will work with the SLT member responsible

for filtering and monitoring and with IT support, and will ensure online risks are considered within wider safeguarding practice.

### **The Governing Board:**

The governing board has overall strategic responsibility for safeguarding, including online safety and the appropriateness of filtering and monitoring. Governors will receive assurance that systems are effective, that the annual filtering and monitoring review and online safety risk assessment have been completed, that actions are recorded, and that emerging risks such as generative AI are appropriately managed.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

### **Head Teacher:**

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The Head Teacher and other designated safeguarding members of staff are ensuring that any online safety incidents and or cyber bullying incidents are logged and dealt with appropriately in line with this policy and the behaviour policy. They are also aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

### **Computing Lead:**

Takes responsibility in establishing and reviewing the school policies for computing and online safety and associated documents

- Ensure that the policy is implemented and that compliance with the policy is actively monitored
- Ensure that all staff are aware of the procedures and requirements in the event of an online safety incident
- Keep up to date with online Safety issues and guidance through liaison Nottinghamshire's Local Authority Schools ICT team and through advice given by agencies such as the Child Exploitation and Online Protection Centre (CEOP)

### **Technical staff:**

Technical staff (ATOM IT) support school with IT, their role includes;

- To report any e-safeguarding related issues to the Head Teacher/DSL
- To support the school in providing a safe technical infrastructure to support teaching and learning
- To ensure that provision exists for misuse detection and malicious attack
- To ensure school's technical infrastructure is secure and is not open to misuse or malicious attack
- To ensure access to the school network is only through an authorised, restricted mechanism
- To keep up to date with online safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- To liaise with the local authority and other appropriate people and organisations on technical issues

- To support the SLT member responsible for filtering and monitoring and the DSL with checks that filtering is working appropriately on all internet-connected devices in all relevant locations; to keep a record of those checks; and to report any misuse, attempted misuse, alerts or gaps promptly to the Headteacher/DSL.
- To take responsibility for the security of the school ICT system, and review the security regularly
- To ensure virus protection is updated regularly
- To ensure appropriate back up 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 are restricted

### **Managing emerging technologies**

The school will examine emerging technologies, including generative AI, for educational benefit and safeguarding impact before use. Decisions will take account of KCSIE 2026, DfE Generative AI in Education guidance, the DfE Generative AI: product safety standards, filtering and monitoring requirements, data protection, intellectual property, age restrictions and the needs of pupils including those with SEND.

### **Generative AI**

- Any use of generative AI with pupils will be specifically risk assessed, age-appropriate, purposeful and supervised by staff. Pupils will not use open-access AI tools where provider age restrictions are not met.
- AI products will only be introduced where the school is satisfied that appropriate safeguards are in place, including effective content filtering/moderation, monitoring and reporting, security, privacy and data protection, clear intended use, age/SEND considerations, and appropriate human oversight. Where high-risk personal-data processing is proposed, the school will consider whether a Data Protection Impact Assessment is required.

Pupils will be taught, at an age-appropriate level, that AI-generated material may be inaccurate, biased, misleading or manipulated. They will be taught not to share personal information with AI systems and to seek help from a trusted adult if AI-generated content is worrying, unsafe or inappropriate.

### **Annual Risk Assessment**

The DSL, the SLT member responsible for filtering and monitoring and relevant IT support will lead an annual online safety risk assessment. The assessment will reflect the actual risks faced by the school's pupils, including age, SEND and other vulnerabilities, patterns of technology use and emerging risks.

- Identify and evaluate new and emerging risks, including generative AI, AI-generated imagery/deepfakes, misinformation and disinformation, online grooming and exploitation, self-harm/suicide content, radicalisation/extremism, harmful online challenges and scams.
- Inform updates to filtering and monitoring, curriculum, staff training, acceptable-use arrangements, parental information and safeguarding procedures.
- Be reported to governors, with actions recorded and followed up as part of safeguarding and curriculum review.

---

## Staff Training

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. Governors and relevant volunteers receive training appropriate to their role. From September 2026, updates will reflect KCSIE 2026, revised RSHE guidance, generative AI risks and safe use, AI-generated imagery/deepfakes, cyber security, current data protection requirements and emerging online harms.

- Emerging digital risks, including generative AI interactions, AI-generated explicit imagery/deepfakes, misinformation/disinformation, online grooming and exploitation, harmful online content and scams.
- The safe procurement and use of educational technology, including generative AI, with attention to filtering/monitoring, security, privacy, data use, age restrictions and human oversight.

---

## Procurement and Use of Technology

Before introducing new technology, particularly online platforms or generative AI, the school will assess safeguarding, filtering and monitoring, cyber security, privacy/data protection, accessibility, age restrictions and educational purpose. Procurement decisions will be informed by current DfE digital and technology standards and, where relevant, the Generative AI: product safety standards.

- Providers must demonstrate compliance with safeguarding, safety, and data protection requirements.
- Teachers must retain oversight of how tools are used and outputs evaluated.
- Any risks identified must be addressed in advance of implementation.

---

## RSHE Curriculum

Online safety will be embedded across computing, Relationships Education/Health Education and wider safeguarding education. The revised statutory RSHE guidance effective from 1 September 2026 requires primary pupils to learn about respectful online interaction, critical evaluation of online relationships and information, risks from people they have never met, minimum ages for social media, privacy and location settings, the permanence/circulation of online material, harmful content and contact, and how to report concerns and seek help. Teaching will be age- and stage-appropriate, inclusive and responsive to pupils' needs and vulnerabilities. It will reinforce that abuse is never the child's fault, and that pupils should keep seeking help until they are heard. Parents will be informed in line with the school's RSHE arrangements and statutory guidance.

-

### Filtering and Monitoring

Appropriate filtering and monitoring systems are in place to limit pupils' exposure to harmful online material. In line with KCSIE 2026, the school will ensure that a review of their effectiveness is carried out at least once every academic year. The review will be led by the SLT member responsible for filtering and monitoring, with support from the DSL and IT support, and will involve the responsible governor.

- Checks will confirm that filtering works appropriately on all internet-connected devices in all relevant locations. The school will keep a written record of checks, findings, decisions and actions.
  - The review will consider the age range and risk profile of pupils, including pupils with SEND and other vulnerabilities; how and where technology is accessed; the risk of over-blocking; and whether systems can appropriately address real-time, dynamic, personalised and AI-generated content.
  - The leadership team and relevant staff will understand the systems in place, how monitoring alerts are handled and how concerns are escalated. Governors will receive assurance on the review and any required improvements.
- 

ATOM IT support the school's filtering and monitoring arrangements and provide relevant usage/alert information, including blocked or inappropriate searches, to authorised school leaders. Any proposed changes to filtering must be risk assessed and appropriately authorised. The school will maintain oversight of provider performance and will not rely on the technical provider alone to discharge its safeguarding responsibilities. Filtering and monitoring arrangements will be reviewed against the current DfE Filtering and Monitoring core standard.

Any filtering or monitoring alert that gives rise to a safeguarding concern will be considered promptly by the DSL or deputy and recorded on the school's safeguarding system in line with the Child Protection/Safeguarding Policy.

### 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, appropriately filtered broadband and monitoring provision supported by ATOM IT, reviewed against current DfE filtering and monitoring standards.
- Monitoring arrangements that are capable of identifying inappropriate or concerning activity, including content associated with safeguarding and Prevent risks, with clear procedures for review and escalation of alerts.

### Teaching and Support Staff:

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices and implement them consistently
- They report any suspected misuse or problem to the Head Teacher/DSL for investigation, action or sanction
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using the agreed school procedure

- Online safety awareness is embedded in all aspects of the curriculum and other activities and is regularly revisited

They will only use school-approved online platforms and AI tools with pupils and will follow school requirements for age restrictions, supervision, personal data, safeguarding, filtering/monitoring and reporting concerns.

- They monitor the use of digital technologies, including, but not limited to laptops, i-pads and cameras in lessons and other school activities where allowed and implement current policies with regards to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

#### **Parents/carers:**

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way

'Parents/carers often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report 2008)

Butler's Hill Infant and Nursery School will take opportunities to help parents understand online safety through parents' evenings, newsletters, Class Dojo, the school website and relevant campaigns. Information may include age restrictions, privacy and location settings, social media and gaming risks, screen time, harmful content/contact, scams, generative AI and how to report concerns.

Parents and carers will be encouraged to support the school in promoting good online safety practice. Parents and carers role is;

- 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 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.

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

What are the issues? - [UK Safer Internet Centre](#)

Hot topics - [Childnet International](#)

Parent factsheet - [Childnet International](#)

Parental controls - [NSPCC](#)

App Reviews - [Common Sense Media](#)

Online safety for young people - [Childnet](#)

## Teaching and Learning

### Why internet and digital communications are important:

- The purpose of any technology in school is to raise educational standards, to promote achievement to support the professional work of staff and to enhance the school's management functions
- The school has a duty to provide students with quality internet access as part of their learning experience
- Internet use is part of the statutory curriculum and a necessary tool
- They will be taught what internet use is acceptable, and what is not, and be given clear objectives for its use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self-efficacy and resilience

## Education and Curriculum

At Butler's Hill we establish a carefully sequenced, age-appropriate online safety curriculum that builds on prior learning and responds to emerging risk. From September 2026 this is aligned with the revised statutory RSHE guidance as well as the computing curriculum and KCSIE 2026.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

The Online Safety Act 2023 creates duties for regulated online services to tackle illegal content and protect children from harmful content. Ofcom's child-safety regime is relevant to the online environments pupils may use. The school will use this wider legal context to support education for pupils and parents, while recognising that the school's own safeguarding duties under KCSIE remain separate and continue to apply.

The strongest protections in the Act have been designed for children and will make the UK the safest place in the world to be a child online. Platforms will be required to prevent children from accessing harmful and age-inappropriate content and provide parents and children with clear and accessible ways to report problems online when they do arise.

The Act's duties apply to search services and services that allow users to post content online or to interact with each other. This includes a range of websites, apps and other services, including social media services, consumer file cloud storage and sharing sites, video sharing platforms, online forums, dating services, and online instant messaging services.

Protecting children is at the heart of the Online Safety Act. Although some content is not illegal, it could be harmful or age-inappropriate for children and platforms need to protect children from it.

Companies with websites that are likely to be accessed by children need to take steps to protect children from harmful content and behaviour.

The categories of harmful content that platforms need to protect children from encountering are set out in the Act. Children must be prevented from accessing Primary Priority Content, and should be given age-appropriate access to Priority Content. The types of content which fall into these categories are set out below.

#### **Primary Priority Content**

- pornography
- content that encourages, promotes, or provides instructions for either:
  - self-harm
  - eating disorders or
  - suicide

#### **Priority Content**

- bullying
- abusive or hateful content
- content which depicts or encourages serious violence or injury
- content which encourages dangerous stunts and challenges; and
- content which encourages the ingestion, inhalation or exposure to harmful substances.

At Butler's Hill, online safety is taught throughout each year group within our computing curriculum through explicit lessons, and embedded within our curriculum. Pupils are made aware of the impact of cyber bullying during assemblies, stories, safer internet day, PSHE sessions and anti bullying week.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

If a pupil comes across any content online that they find distressing or upsetting, they should follow the school SMART code and tell a trusted adult immediately. 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.

Pupils will;

- Know and understand school policies regarding cyber bullying
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- 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
- 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

## **Cyber Bullying**

Cyber-bullying takes place online, for example through messaging, social media, gaming or other digital services. Online child-on-child abuse may also include abusive or discriminatory messages, the consensual or non-consensual making or sharing of nudes/semi-nudes, AI-generated explicit images or deepfakes, and sharing harmful sexual or violent content. All such concerns will be treated as safeguarding matters and responded to in line with the school's safeguarding and behaviour procedures.

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

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets and regularly updates the Online Safety section of the school website on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

## **Uses of Technology**

### **E-mail via Outlook**

All members of staff have a strict code of conduct to which they must adhere. Under no circumstances must staff give out their personal email address or contact details to parents/carers or pupils. Any correspondence via email or any other application should be via the

school email accounts.

### **Published content and the school website**

Our school website is partially open and can be universally accessed requiring no user name or password. All staff are responsible for monitoring the site and subject/ year group leader are responsible for their class page. It is the duty of all users to ensure that appropriate material is uploaded. In the unlikely event of any inappropriate material appearing it should be reported directly to the Head Teacher who will take the necessary action. No staff or pupil's personal details will be published.

### **Publishing pupils' images and work on the school website, and other platforms**

- Written permission will be obtained from parents and carers before any photographs are published on the school website or other platform.
- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified.
- Pupil's full names will not be used on the school website and other learning platforms.
- Parents should be clearly informed of the school policy on image taking and publishing when joining school, or if there are any updates.

### **Managing emerging technologies**

The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.

### **Blended/Remote Learning**

This policy alongside our ICT policy will be used to support staff and parents support pupils to access any remote/blended online learning safely. The school will examine emerging technologies, online platforms, video links etc for their educational benefit and carry out a risk assessment to ensure the delivery and the way children access them support Safe Guarding and GDPR guidelines before use in school/home.

### **Mobile phones and personal devices**

In line with KCSIE 2026, the school is a mobile phone-free environment for pupils by default. Pupils should not have access to mobile phones during the school day unless an individual exception has been authorised for a specific need. Staff, visitors and parents must follow school rules on personal-device use, photography and safeguarding in areas where children are present.

### **Protecting personal data**

Personal data will be processed in accordance with the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025, together with current DfE data protection guidance for schools. This includes data processed through online platforms, monitoring systems and generative AI tools.

This section of the policy offers clear guidance to users regarding the management of potentially sensitive data. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purpose
- Kept no longer than necessary
- Only transferred to others with adequate protection

At Butler's Hill Infant and Nursery School, data is kept secure and all staff are informed as to what they can and cannot do with regard to data in the following ways;

- Relevant staff know the location of the data.
- Staff with access to personal data understand their legal responsibilities
- School ensure that data is appropriately managed both within and outside the school environment
- All staff are aware they should only use approved means to access, store and dispose of confidential data
- Staff who have remote access to school data must ensure the data remains secure by being aware of the dangers of unsecured wireless access outside school

#### **Mobile devise and removable media:**

- Devices containing data may be allowed to be removed from the school premises with the knowledge of the head
- Butlers Hill ensures the risk of admin data loss is addressed and managed
- Pupils, parents/carers are not permitted to use any mobile devise on the classroom floor or in areas where there are children

#### **Use of digital media:**

In our school we recognise the safeguarding and data protection issues surrounding digital media. All users will be informed about the risks connected with taking, using, sharing, publishing and distributing images and video and will consider the purpose for which media is used. Photographs and videos of pupils and staff are personal data. Their collection, storage, sharing and publication will be managed in accordance with the Data Protection Act 2018, UK GDPR, the Data (Use and Access) Act 2025 and the school's Data Protection Policy, with an appropriate lawful basis and privacy information.

- Permission will be obtained from parents/carers upon the child entering the school
- School will not re use any photo or videos after 5 years
- Full names and personal details will not be used on digital media, particularly photos
- Staff are aware that photographs/video staff that are taken using school equipment must only be used for school purposes, and only accessible to the appropriate adults/pupils
- Staff must not use their own personal media devices to take photographs or videos
- When taking photographs/ video staff will ensure that all subjects are appropriately dressed and not participating in activities that could be misinterpreted
- Staff/parents/carers and pupils will be educated in the dangers of publishing images and videos of pupils or adults on Social Networking sites or websites without consent of the persons involved
- The guidelines for safe practise relating to the use of digital media, will be monitored by the Head Teacher

#### **Communicating the policy**

##### **Pupils:**

- Appropriate elements of the online safety policy will be shared with pupils
- Online safety rules will be shared with all pupils and displayed where appropriate
- Pupils will be informed that network and internet use will be monitored
- Age-appropriate curriculum opportunities will ensure pupils develop knowledge and skills for online safety. Content will be reviewed regularly in response to KCSIE, RSHE, local

safeguarding intelligence and emerging risks, including generative AI and manipulated media.

**Staff:**

- All staff will have access to this Online Safety Policy and will be expected to read, understand and follow it. Staff will also read KCSIE 2026 Part One in full, as required by KCSIE 2026, and complete relevant safeguarding/online safety training.
- Staff should be aware that the system is monitored and that professional standards are expected.

**Parents/carers:**

- Parents/carers will be notified of the policy in newsletters and the school website
- All parents/carers will be asked to sign the photograph consent when they register their children.

**Illegal Offences**

Any suspected illegal online material or activity, including suspected child sexual abuse material or AI-generated child sexual abuse material, will be brought immediately to the Headteacher/DSL and managed through safeguarding procedures. Staff will preserve evidence where appropriate, avoid unnecessary viewing or sharing, and refer to the police, local authority or other relevant agencies as required. The school will not conduct an independent criminal investigation.

**Some useful websites**

UK Council for Internet Safety (UKCIS) / GOV.UK online safety guidance

CEOP Education / CEOP Safety Centre

CEOP Education (formerly Thinkuknow)

Internet Matters - practical guidance for families

Childline; <http://www.childline.org.uk/>

UK Safer Internet Centre; <http://www.saferinternet.org.uk>

Childnet International; <http://www.childnet.com>

NSPCC online safety advice

NSPCC online safety and safeguarding resources

**Some useful sites for children and young people**

[www.digizen.org](http://www.digizen.org)

[www.chatdanger.com](http://www.chatdanger.com)

[www.kidscape.org.uk](http://www.kidscape.org.uk)

[www.childline.org.uk](http://www.childline.org.uk)

[www.beatbullying.org](http://www.beatbullying.org)

## Don't accept friend requests from pupils on social media

### 10 rules for school staff on Facebook

1. Be careful when displaying your full name to discourage pupils and parents/carers to befriend you on social media sites - we advise to use your first and middle name, use a maiden name, or put your surname backwards
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Be careful what you post and share - once it's out there, it's out there
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online - once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Avoid using Facebook while in the school building. The app can use data location to make friend suggestions (such as parents or pupils)

---

### Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** - go to [bit.ly/2MdQXMN](https://bit.ly/2MdQXMN) to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** - go to [bit.ly/2zMdVht](https://bit.ly/2zMdVht) to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

### What do to if...

#### A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

**You're being harassed on social media, or somebody is spreading something offensive about you**

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a parent, member of staff or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Policy review: September 2026. This policy will be reviewed at least annually and sooner where statutory guidance, technology or the school's risk profile changes.

### **Acceptable Use Agreement: Staff, Governors and Visitors**

This policy is designed to ensure that all staff are aware of their professional responsibilities. All staff are expected to sign this policy and adhere at all times to its contents.

- I have read and understood Butler's Hill Infant and Nursery School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Head teacher (if by an adult).
- I will only use the school's email / Internet / and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents/carers.
- I will only use the approved, secure e-mail system(s) for any school business.

I will only use school-approved AI and online tools for school business and pupil activity, will comply with provider age restrictions and school risk assessments, and will not enter personal, special-category or confidential information into unapproved AI systems.

I understand that AI-generated outputs may be inaccurate, biased, unsafe or infringe copyright, and I will apply professional judgement, verify outputs before use and report safeguarding concerns arising from AI use.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that school systems and users are protected by security, filtering and monitoring services. My use of school devices, systems, accounts and logins may be monitored by authorised staff in accordance with safeguarding, security and data protection requirements, and I will not attempt to bypass these controls.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's online safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

[illegible]

Signature.....Date .....

Name.....Jobtitle.....

Please read the online safety policy and sign to say you have read it

