Online Safety Policy

Agreed: Summer 2025

Review: Summer 2026

Contents

Introduction

The use of Information and Communication Technology (ICT) in the 21st century is an essential resource supporting learning, teaching, and everyday life. The rise in remote learning and increased online activity has further emphasised the importance of equipping children with lifelong digital skills and knowledge.

ICT encompasses a wide range of resources including web-based and mobile learning. The rapid evolution of digital technologies demands continuous adaptation. Children are currently engaging with a variety of platforms and tools, such as:

- Websites
- Learning platforms (e.g., Google Classroom), Virtual Learning Environments (VLEs)
- Email and messaging apps
- Chat rooms and social networks
- Blogs and wikis
- Video broadcasting and livestreaming
- Music and media platforms
- Online gaming
- Smartphones with text, video, and internet capabilities

While these technologies offer significant benefits, they also present a range of risks. At Brigg Primary School, we are committed to educating pupils about online safety, enabling them to act safely, responsibly, and legally when using the internet.

This policy incorporates updates from the **Online Safety Act 2023**, **Keeping Children Safe in Education (KCSIE) 2024**, and best practices from the **NSPCC** and **UK Safer Internet Centre**.

A Whole-School Approach to Online Safety

Online safety is a shared responsibility that involves every member of the school community, including:

- Pupils
- Staff
- Governors
- Parents and carers
- Visitors and volunteers

Responsibilities

Senior Leadership Team (including Designated Safeguarding Lead)

- Promote an online safety culture across the school
- Support the Online Safety Lead
- Provide resources and training for effective online safety implementation

- Review incident logs and ensure procedures are followed
- Integrate online safety into the safeguarding strategy
- Lead on online safety concerns.
- Liaise with external agencies as necessary.

Online Safety Lead / Computing Lead / IT Support

- Develop and maintain online safety policies
- Monitor national guidance and technological trends
- Deliver annual training to all staff; record participation
- Embed online safety into the curriculum, particularly computing and RSHE
- Promote online safety to parents and carers
- Liaise with local safeguarding partners and agencies
- Maintain the online safety incident log
- Ensure robust filtering and monitoring systems are in place and regularly reviewed

Teachers and Support Staff

- Understand and follow online safety policies and AUP
- Model safe and responsible technology use
- Include online safety in lessons
- Supervise pupils during tech use
- Report incidents to DSLs using appropriate systems (e.g., CPOMS)

Pupils

- Understand and follow the pupil AUP
- Learn about the benefits and risks of digital technologies
- Use technology responsibly at school and home
- Report concerns to trusted adults
- Respect others' rights, feelings, and intellectual property

Parents and Carers

- Support the school's online safety approach
- Discuss safe technology use at home
- Monitor children's online activity
- Promote responsible digital habits
- Seek advice from school and national bodies when needed

Governing Body

- Understand and support online safety policies
- Monitor infrastructure safety and incident response
- Ensure adequate funding and resources
- Champion parent and community involvement in online safety

Addressing Online Risks

Brigg Primary School educates pupils about the four key areas of online risk:

- **Content:** harmful or inappropriate material
- **Contact:** interactions with strangers or unsafe individuals
- **Conduct:** pupils' own behaviour online
- **Commerce:** risks of scams, fraud, and commercial exploitation

Filtering and Monitoring

Our school ensures robust filtering and monitoring systems are in place to safeguard pupils online. We use Agilico (O2), which is regularly reviewed and updated in collaboration with our IT provider (**South Farm CPA**). Monitoring includes active review of internet usage and alerts for concerning behaviour. These measures are age-appropriate and proportionate to the level of risk. Governors receive annual reports on the effectiveness of filtering and monitoring arrangements.

The school takes cyber security seriously and follows best practice on data protection, password management, software updates, and phishing awareness. Staff receive training in recognising cyber threats. The school works closely with its IT provider to maintain secure systems and respond to incidents.

Teaching and Learning

• We will provide a series of specific online safety-related lessons in every year group/specific year groups as part of the computing curriculum / PSHE curriculum / other lessons.

• We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

• We will discuss, remind or raise relevant Online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials. (Including relevant issues, such as 'sexting')

• We will remind pupils about their responsibilities through an AUP which every pupil will sign.

• Staff will model safe and responsible behaviour in their own use of technology during lessons.

Computing Curriculum

Pupils will be taught about online safety as part of both the computing curriculum and the PSHE/RHE curriculum:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Learning technologies in school

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

	Pupils	**Staff**
Personal mobile phones brought into school	Allowed with permission and stored by staff during school day	Allowed
Mobile phones used during lessons	Not allowed	Not allowed
Mobiles phones used outside lessons	Not allowed	Allowed
School mobile on trips	Not allowed	Allowed
Taking photographs / video on personal equipment	Not allowed	Allowed only in school trips *photos to be backed up to school google photo account / laptop and removed from device as soon as possible.
Taking photographs / video on school devices	Allowed with permission * any images published with parents permission (annual consent form)	Allowed * any images published with parent's permission (see annual consent form)
Use of hand held devices, such as PDAs, MP3 players or personal gaming consoles	Allowed with permission *School equipment only	Allowed

Use of personal email addresses in school	Not allowed	Allowed (outside teaching hours)
Use of school email addresses	Allowed with permission (via school domain gmail account)	Allowed (via school domain @briggprimary.co.uk or @northlincs.gov.uk account)
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed except as part of a planned teacher led activity	Not allowed except as part of a planned teacher led activity
Use of blog, wikis, podcasts or social networking sites	Allowed with supervision	Allowed *Only school accounts, eg Class Dojo, Twitter
Use of video conferencing	Allowed with permission (Google Meet)	Allowed with permission (Google Meet internal / others from outside agencies links)

Using email

• Staff and pupils should use approved e-mail accounts allocated to them by the school (@briggprimary.co.uk), and be aware that their use of the school e-mail system may be monitored and checked.

• Pupils may be allocated e-mail accounts/addresses for their use in school under supervision of the class teacher. Classes may be allocated (@briggprimary.co.uk) email address as required, linked to curriculum coverage in enable local, national or global links.

• Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.

• Staff and pupils are not permitted to access personal e-mail accounts (on staff machines) during school hours

• Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

• Any inappropriate use of the school VLP or e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

The school will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Digital images, video and sound will only be created using equipment provided by the school and for school related activities.

• In particular, digital images, video and sound will not be taken without the permission (as per annual consent forms) 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/pupils involved.

• If pupils are involved, relevant parental permission will also be sought before resources are published online (Home/School agreement booklet).

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

• Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website and will be monitored by the Online Safety Lead. School Twitter accounts and Facebook pages will be managed by the members of the SLT and managed access may be provided to other members of staff.

• Pupils 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. Pupils will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.

• 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 of school.

Using mobile phones

• Staff phones should be turned off or on silent and be stored away from pupils. Calls should be made / received in private, during non-contact time.

• KS2 Pupils can bring mobile phones to school, but must be handed in to a member of staff, who will store the securely until home time.

• Where staff members are required to make phone call for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, staff will not be expected to use their personal mobile phones in any situation (where their mobile phone number or other personal details may be revealed to a pupil or parent.)

Staff should contact the school office, who will then contact the relevant people.

(See Emergency Plan for additional information regarding use of personal mobiles)

Mobile phones are a common vehicle for cyberbullying, through the recording of inappropriate images or video, distributing such images and videos via Bluetooth or other wireless technologies, or the sending of abusive text messages. The school has referred to cyber bullying in the Anti-Bullying policy.

Responding to Emerging Technology and AI

• The school is committed to reviewing and responding to emerging technologies and online trends that may pose risks to pupils. This includes AI-generated content, deepfakes, and new forms of social media.

• The DSL and SLT will regularly assess new risks and adapt training, curriculum, and monitoring accordingly.

Protecting personal data

• The school will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 (Business Manager main contact).

• Staff will ensure they properly log-off from a computer terminal after accessing personal data. During inactivity devices should be 'locked'

- Passwords should be secure (8 characters long, combination of upper/lowercase letters/numbers.
- External hard drives should be encrypted.
- School laptops and devices should not be shared with friends or friends.

• Staff will not remove personal or sensitive data from the school premises without ensuring such data is kept secure, using encrypted devices only. Passwords for cloud services (eg Scholar Pack / Otrack)

• School iPads must be set up with the school staff passcode to ensure data protection.

The school website and other online content published by the school

• The school website/app will not include the personal details, including individual e-mail addresses or full names, of pupils.

• A generic contact form will be used for all enquiries received through the school website which will forward messages to the office.

• Individual staff email addresses may be published on the website/school app

• All content included on the school website, school app and social media posts will be checked by the SLT.

• The content of the website will be composed in such a way that individual pupils cannot be clearly identified.

• Staff and pupils should not post school-related content on any external website without seeking permission first.

Incident Reporting and Response

Online safety incidents are reported to the DSL and recorded in safeguarding software. Incidents are investigated promptly with appropriate actions taken, including referral to external agencies if necessary.

Dealing with Online Safety Incidents

All online safety incidents must be reported immediately to the Headteacher, Designated Safeguarding Lead (DSL), and Online Safety Lead. All staff must follow the procedures outlined below, in line with KCSIE and local safeguarding arrangements.

Children must feel confident that they can report online safety incidents in a no-blame culture, without fear of reprisal.

Unintentional Access to Inappropriate Websites

- Stay calm; avoid overreaction.
- Report to the Headteacher and DSL.
- Decide whether to inform the child’s parents/carers.
- Notify the IT technician or filtering provider to block future access.
- Escalate to the LA if filtering is provided via the LA/RBC.

Intentional Access by a Child

- Refer to the school’s Acceptable Use Policy (AUP).
- Apply agreed sanctions where appropriate.
- Inform the child’s parents/carers.
- Notify technical support to block access if needed.
- Review filtering settings; escalate to the LA if appropriate.

Inappropriate Use of IT by an Adult

- Always involve a second adult; never investigate alone.
- Report immediately to the Headteacher and DSL.
- Restrict further access to the device.
- If the material is offensive but not illegal:
- - Secure the device in a locked location.
- - Conduct a full audit of school IT systems.
- - Record and review the materials involved.
- - Take appropriate disciplinary action (liaise with HR).
- - Refer to the Local Authority Designated Officer (LADO).
- - Inform the Governing Body.
- If material may be illegal:
- - Contact the police or relevant cybercrime unit.
- - Follow all instructions from authorities and log all actions.

Bullying via Email or Mobile Devices

- Advise the child not to respond.
- Refer to anti-bullying, safeguarding, and online safety policies.
- Preserve any evidence (e.g., screenshots, message logs).
- Inform the child's parents/carers.
- Report to email or mobile service provider.
- Involve police if necessary.
- Inform the LA Online Safety Officer.
- Consider delivering a parent workshop.

Malicious Online Comments about a Pupil or Staff Member

- Contact the site admin to request removal.
- Preserve and record all evidence.
- Report to CEOP if grooming or exploitation is suspected: https://www.ceop.police.uk/safety-centre
- Report to police if appropriate.
- Inform the LA Online Safety Officer.

Suspected Grooming or Inappropriate Online Contact

- Report to the DSL immediately and inform parents/carers.
- Advise the child to block the contact and save all communications.
- Report to CEOP and consider police/social care involvement.
- Record on the school safeguarding system (e.g. CPOMS).
- Inform the LA Online Safety Officer.
- Consider a parent information session for the wider school community.

Staff Training

All staff receive online safety training as part of their induction and ongoing CPD. This includes recognising online harms such as grooming, radicalisation, online sexual abuse, cyberbullying, and emerging threats such as AI-generated content and harmful gaming behaviour. Training is updated regularly and tailored to staff roles. CPD is provided by National College

Prevent Duty and Online Radicalisation

Our filtering and monitoring systems are designed to identify indicators of radicalisation, extremism, or grooming. Staff are trained to recognise the signs and respond promptly. The school promotes critical thinking and resilience against extremist content through its curriculum and pastoral support.

Parental Engagement

The school works closely with parents and carers by:

- Providing regular updates on online safety topics
- Hosting workshops and information sessions
- Sharing resources from trusted organizations like the NSPCC and UK Safer Internet Centre

Useful Websites:

UK Government & National Guidance

- **Keeping Children Safe in Education (KCSIE)**
  Statutory guidance that schools must follow when carrying out their duties to safeguard and promote the welfare of children.
- **UKCIS (UK Council for Internet Safety)**
  Offers frameworks, guidance, and best practices for online safety education.
- **Education for a Connected World Framework**
  Framework to support the development of children and young people's understanding of online safety.

Child Protection & Safeguarding Organisations

- **NSPCC – Online Safety**
  Comprehensive advice and resources for schools, parents, and carers.
- **Childnet International**
  Resources for children, teachers, and parents to support safer internet use.
- **Internet Matters**
  Practical guides for teachers and families, plus policy resources.
- **CEOP (Child Exploitation and Online Protection)**
  Reporting tool and safety education for children about exploitation and abuse online.

Schools-Focused Support

- **SWGfL (South West Grid for Learning)**
  Includes template policies, toolkits (e.g. Online Safety Policy Template), and training tools such as the 360° Safe self-review tool.
- **National Online Safety (NOS)**
  CPD-accredited training, policy templates, and regular online safety updates for schools.
- **ProjectEVOLVE**
  Online safety resources mapped to the Education for a Connected World framework.

Technical and Filtering Guidance

- **UK Safer Internet Centre – Filtering and Monitoring Guidance**
  Specific requirements and recommendations for filtering and monitoring systems.
- **LGfL (London Grid for Learning)**
  Online safety resources, policy templates, and curriculum tools.

Policy Review

This policy is reviewed annually by the Online Safety Lead and DSL in consultation with staff, governors, and safeguarding partners. Updates reflect changes in DfE guidance and online risk trends.

Staff and Pupil Acceptable Use Policies (AUPs)

Acceptable Use Policy - Staff

This policy covers the use of digital technologies in school: i.e email, internet, intranet and network resources, learning platform, software, mobile technologies, systems equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the school approved, secure email system(s) for any school business i.e. @briggprimary.co.uk and @northlincs.gov.uk email.
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/school named contact: Mrs Winter.
- I will not allow unauthorised individuals to access email/internet/intranet/network, or other school/LA systems.
- I will ensure that all my secure login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself.
- I will not download any software, apps or resources from the internet that can compromise the network, or are not adequately licensed.
- I will follow the guidance in the People who work with Young People document and ensure that my personal email accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I understand that all internet usage/and network usage can be logged and this information could be made available to my manager upon request.
- I will ensure that all documents are labelled, saved, accessed and deleted in accordance with the school's network security and confidentiality protocols, which ensure minimum mandatory compliance with the Cabinet Officer Data handling Procedures in Government : www.cabinetoffice.gov.uk/reports/data_handling.aspx
- I will not connect a computer, laptop or other device, to the network/internet that has not been approved by the school and meets its minimum security specification (i.e. up to date approved Anti virus etc.)
- I will ensure that any private social networking sites/blogs etc that I create or actively contribute to are not confused with my professional role.
- I will not engage in any online activity that may compromise my professional role this includes any comments made on personal social media messaging platforms.

- I agree and accept that any computer / laptop / mobile device loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any software, apps or device relating to personal use to ensure that it does not breach the school policies.
- I will ensure any confidential information that I wish to transport from one location to another is protected by encryption, using the school USB drives.
- Mobile phones, mobile devices and the internet should not be accessed on site in a personal capacity with children present
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within any schools system (e.g. MIS, Learning Platforms etc), will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safeguarding issues so that they are appropriately embedded in my classroom practice.
- I will only use LA systems in accordance with any corporate policies.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

User Signature

- I understand that it is my responsibility to ensure that I remain up to date and read and understand the schools most recent Acceptable Use Policy (normally an annual revisit).
- I agree to abide by the schools most recent Acceptable Use Policy.
- I wish to have an email account; be connected to the intranet and internet; be able to use the schools ICT resources and systems.
- I understand that all my activity and usage of the school ICT system can be monitored and information on such activity and usage can be accessed and actioned upon to safeguard myself and others.

Signature……………………………………………………………………………………………………

Date……

Full Name…………………………………………………………………………………………………..

Job Title……………………………………………………………………………………………………..

School………………………………………………………………………………………………………

Professionals' Online safety Agreement

Inc Students, Parent Helpers and Volunteers

- In line with the school's Safeguarding and Online safety policies any visitors to school need to agree to the following statements.
- I will not use my personal mobile phone or similar devices whilst in the presence of children or within the school building between the hours of 8.45am and 3.45pm. The school's telephone number can be given as a point of contact if out of the school building.
- I will not use personal digital cameras or camera phones.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to will not contain any information regarding school activities, children or their behaviour.
- I will notify staff immediately if I hear or see anything of a confidential nature and any information will not be discussed outside of school. I will not discuss any children or their behaviour, with anyone outside of school.

Signature ____

Date ____

Full Name ____