Brookland Infant and Nursery School

Online Safety Policy

Name of School	**Brookland Infant and Nursery School**
Policy review Date	**17/12/2025**
Date of next Review	**17/12//2026**
Who reviewed this policy?	**Safeguarding committee**

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

1.1 Introduction and Overview

Rationale

We recognise that the Internet offers great experiences for adults and children. There are opportunities to improve your life, have some fun, enhance your education or pursue business interests. Children are often enthusiastic internet users - particularly of interactive services and social media. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. This policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE) focusing on teaching pupils about misinformation, disinformation and conspiracy theories. We have updated this policy in line with the DFE's guidance about the use of generative AI in education settings and filtering and monitoring standards. This policy has also been updated to integrate the principles outlined in our safe use of AI Policy. It has been reviewed by Forbes Solicitors LLP in line with government legislation and guidance for the academic year 2025/2026. It is designed to sit alongside or be integrated into the school's statutory Child Protection and Safeguarding Policy. Any issues and concerns with online safety follow the school's safeguarding and child protection procedures.

Why is internet use important?

The purpose of internet use in school is to raise educational standards, to promote children's achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Our Computing curriculum is tailored to provide a rich, engaging and memorable programme of study for our children and computing and online resources are increasingly used across the curriculum to enhance learning experiences. This enables our children to work creatively and collaboratively.

Online safety in the curriculum

We believe it is essential for online guidance to be given to the children on a regular and meaningful basis. Online safety is taught throughout the school year, through all year groups and is focused on discretely in KS1 as part of their weekly Computing lessons. We continually look for new opportunities to promote online safety throughout the school and to the Brookland community.

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Brookland Infant and Nursery School with respect to the use of IT-based technologies
- safeguard and protect the children and staff of Brookland Infant and Nursery School
- 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
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use

- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- 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
- minimise the risk of misplaced or malicious allegations made against adults who work with children and students.
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. PSHE) and beyond.

Main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content
- Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate content
- content validation: how to check authenticity and accuracy of online content

Contact

- Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- social or commercial identity theft including passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (e.g. amount of time spent online)
- sexting (sending and receiving of personally intimate images)
- copyright (little care or consideration for intellectual property and ownership).
- Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1.3 Scope

This policy applies to all members of Brookland Infant School community (including staff, children, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of Brookland Infant IT systems, both in and out of our school.

1.4 Roles and responsibilities

Role	Key Responsibilities
Headteacher	• adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • take overall responsibility for online safety provision • take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles and to train other colleagues, as relevant • aware of procedures to be followed in the event of a serious online safety incident • ensure suitable 'risk assessments' undertaken so the curriculum meets needs of children, including risk of children being radicalised • receive regular monitoring reports from the IT company • ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • ensure that parents/carers are kept informed of any relevant national concerns about online safety • be the LGfL nominated contact and ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts • ensure school website includes relevant information.
Designated Safeguarding Lead	• take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • promote an awareness and commitment to online safety throughout the school community • ensure that online safety education is embedded within the curriculum • to communicate regularly with SMT and the Designated Safeguarding Governor/committee to discuss current issues, review incident logs and filtering/change control logs

Role	Key Responsibilities

	• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• ensure that online safety incidents are logged as a safeguarding incident
	• facilitate training and advice for all staff
	• liaise with the Local Authority and relevant agencies
	• regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues which might arise from:
	  • sharing of personal data
	  • access to illegal/inappropriate materials
	  • inappropriate online contact with adults/strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors/ Safeguarding Governor	• read, understand and help promote the school's online safety policies and guidance • to ensure that the school follows all current online safety advice to keep the children and staff safe and regularly review this with the computing leader • to recommend the Online Safety Policy to the relevant committee and the Governing Body and review its effectiveness • support the school in encouraging parents and the wider community to become engaged in online safety activities.
Computing Curriculum Leader	• actively promote an awareness and commitment to online safety throughout the school community • oversee the delivery of the online safety element of the Computing curriculum • liaise with the school ICT technical support staff.
Business Manager	• ensure that the data they manage is accurate and up-to-date • ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements • ensure the school is registered with the Information Commissioner.
Technician	• report any online safety related issues that arises to the Designated Safeguarding Lead • ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • ensure the security of the school ICT system • ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • ensure the school's policy on web filtering is applied and updated on a regular basis • ensure that LGfL is informed of issues relating to the filtering applied by the Grid ensure that he/she keeps up-to-date with the school's online safety policy and technical information in order to effectively

Role	Key Responsibilities
	carry out their online safety role and to inform and update others as relevant • ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • keep up-to-date documentation of the school's online security and technical procedures • ensure all LGfL services are managed on behalf of the school following data handling procedures are relevant.
Teachers	• read, understand and follow the school's Online Safety Policy, Home School Acceptable Use Agreement, Blended Learning Policy • read, understand, sign and adhere to the school staff Acceptable Use Policy Agreement • embed online safety issues in all aspects of the curriculum and other school activities • model safe, responsible and professional behaviours in their own use of technology • supervise and guide children carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities if relevant) • ensure that children are aware of research skills and are aware of legal issues relating to electronic content such as copyright laws, where appropriate.
All staff, volunteers and contractors	• read, understand and help promote the school's online safety policies and guidance • read, understand, sign and adhere to the school staff Acceptable Use Policy Agreement • report any suspected misuse or problem to the Designated Safeguarding Lead • maintain an awareness of current online safety issues and guidance e.g. through CPD • model safe, responsible and professional behaviours in their own use of technology • return any equipment or devices loaned by the school at the end of the period of employment/volunteering. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Children	• to read, understand, sign and adhere to the Home – School Acceptable Use Agreement (parents/carers can sign on behalf of the children if needed) • understand the importance of reporting abuse, misuse or access to inappropriate materials • know what action to take if they or someone they know feels worried or vulnerable when using online technology • know and understand school policy on the use of school devices e.g. digital cameras, iPads, chromebooks and laptops

Role	Key Responsibilities
	• understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school. • help the school in the review of online safety policies by contributing to any 'pupil voice' / surveys that gathers information of their online experiences.
Parents / carers	• read and understand the school Online Safety Policy, Blended Learning Policy • read, understand, sign and follow the Home - School Acceptable Use Agreement • support the school in promoting online safety and endorse the Home – School Acceptable Use Agreement which includes the children's use of the Internet and the school's use of photographic and video images • contact the school if they have any concerns about their child/ren's use of technology.
External groups	• any external individual/organisation will sign our Acceptable Use agreement prior to using technology or the Internet within school • support the school in promoting online safety • model safe, responsible and positive behaviours in their own use of technology.

1.5 Communication

The policy will be communicated to staff/children/community in the following ways:

- Policy to be posted on the school website and be accessible on the staff shared area
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and children at the start of each year. Home – School Acceptable Use Agreements to be issued to whole school community, on entry to the school.

1.6 Handling Incidents

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Members of staff are given information about infringements in use and possible sanctions. Sanctions available include:

- referral to Headteacher – warning given
- referral to Headteacher/Governors and follow school disciplinary procedures
- report to the LADO
- referral to the Police.

Children are given information about infringements in use and possible sanctions. Sanctions available include:

- referral to Headteacher – warning given
- informing parents or carers
- removal of Internet or computer access for a period of time
- referral to the Police.

The Designated Safeguarding Officer acts as first point of contact for any incident and Online Safety incidents will be logged. Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school safeguarding procedures. Please also refer to the school Complaints Procedure.

1.6.1 Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

Whether there is an immediate risk to a young person or young people

When assessing the risks the following should be considered:

  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the children involved - in most cases parents should be involved.

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply, then school may decide to respond to the incident without involving the police or children's social care (school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to children involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

1.7 Reviewing and Monitoring Online Safety

The Online Safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE and Computing policy).

This policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. Shared with all staff and at an appropriate level with children. All amendments to the school online safety policy will be disseminated to all stakeholders.

2. Education and Curriculum

2.1 Child online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy
  - to begin to understand that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be
  - to begin to understand how search engines work and to understand that this affects the results they see at the top of the listings
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
  - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and

videos and to know to ask for adult support to ensure they have turned-on privacy settings
  - to understand why they must not post pictures or videos of others without their permission
  - to know not to download any files – such as music files
  - to have strategies for dealing with receipt of inappropriate materials
  - to understand not all information, they find on the internet is real and introduce the idea that some information is real and some is fake. Discuss ways they may be able to determine this.
  - to know how to report any abuse including cyberbullying; and how to seek 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 CLICK CEOP help button.

- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology during lessons, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that when copying materials from the web, staff and children understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights; only support legal downloading of music from an appropriate site (LGFL audionetwork)
- ensures children only use school-approved systems and publish within appropriately secure / age-appropriate environments, e.g. Purple Mash, Busy things

2.2 Staff and governor training

This school:

- makes regular training available to staff and governors on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements
- ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

2.3 Parent awareness and training

This school runs a rolling programme of advice, guidance and training for parents, including:

- providing Home-School Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
- annual parent meeting for online safety advice, guidance and training for parents
- information in school newsletters/ Arbor
- suggestions for safe Internet use at home via Weekly Newsletters
- provision of information about national support sites for parents.
- Ad hoc events or speakers

3. Expected Conduct and Incident management

3.1 Expected conduct

All users:

- are responsible for using the school IT systems in accordance with the relevant Acceptable Use Agreements and guidance
- understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good online safety practice when using digital technologies out of school
- know and understand school policies on the use of mobile and hand held devices including cameras. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

Members of staff, volunteers and contractors:

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices
- know to be vigilant in the supervision of children at all times, as far as is reasonable
- know to take professional, reasonable precautions when working with children, previewing websites before use; using online appropriate (child friendly) search engines where more open Internet searching is required with younger children and inform children that internet usage is monitored.

Parents/carers:

- are required to provide consent for children to use the Internet, as well as other technologies, as part of the Home-School Acceptable Use Agreement signed at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

3.2 Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions
- all members of the school and wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issue monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- staff and children must report any inappropriate sites or images not filtered via our filtering system to the Headteacher
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- a member of the designated safeguarding team will contact the Police if a member of staff or child receives online communication that we consider is particularly disturbing or breaks the law. A member of the designated safeguarding team will

immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the IT and Communication System

The DSL has now been asked to take lead responsibility for web filtering and monitoring, marking a clear shift. Schools now need to follow the new DfE standards and consider the roles and responsibilities of all staff – for DSLs and SMT, the challenge is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams. All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about over blocking or gaps in the filtering provision. Schools will also be reviewing their approaches to monitoring in line with the standards (note that filtering and monitoring are not the same – there is guidance around this for DSLs at https://safefiltering.lgfl.net)

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

Staff can submit concerns by speaking to one of the safeguarding team directly. Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. It is very important that schools understand the difference between filtering and monitoring, the meaning of over blocking and other terms, as well as how to get the best out of our systems.

4.1 Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is filtered and monitored
- As an LGFL school, we do have filtering and monitoring in place. This is provided by the LGFL, and it is called **WebScreen** version 3. It was recently upgraded from version 2 by the LGFL (see webscreen privacy policy)
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. pornography, race hate, gaming, sites of an illegal nature). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status; Computing Leader, Headteacher and Badger/ Croft IT staff
- uses USO user-level filtering where relevant
- ensures network health through use of Sophos anti-virus software (from LGfL)
- uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- is vigilant in its supervision of children's use at all times, as far as is reasonable.

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or

inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

4.2 Network management (user access, backup)

This school:

- uses individual, audited log-ins for all users - the LGfL USO system
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful
- has additional local network monitoring/auditing software installed;
- ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies
- has daily back-up of school data (admin and curriculum)
- uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance (Google Drive)
- storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a username and password for access to our school's network
- has a separate shared network for staff and children
- provides all children with a class/ individual username and password which gives them access to the Internet and other services
- provides all children have an individual username and password which gives them access to Purple Mash, EdShed (Year 2) and MyMaths
- makes it clear that no one should log on as another user and makes clear that children should never be allowed to log-on or use teacher and staff logins
- has set-up the network with a shared work area for children and one for staff. Staff and children are shown how to save work and access work from these areas
- requires all users to log off when they have finished working or are leaving the computer unattended
- ensures all equipment owned by the school and/or connected to the network has up to date virus protection
- makes it clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used to support their professional responsibilities
- makes it clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email, finance system, personnel system etc.
- maintains equipment to ensure Health and Safety is followed

- ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- has a clear disaster recovery system in place that includes a secure, remote off site back up of data
- uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.
- ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA
- our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- ensures all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. At Brookland Infant and Nursery School this includes: Google Drive and Purple Mash (children). For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Brookland Infant and Nursery has a clear GDPR policy which staff, governors and volunteers must follow at all times

4.3 Passwords

This school:

- ensures that all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private
- ensures that all staff and children know they must keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately
- requires staff to use STRONG passwords
- requires staff to change their passwords into the MIS, LGfL USO admin site, at least twice a year
- requires staff to use critical systems to use two factor authentication.

4.4 E-mail

This school

- provides staff with an email account for their professional use and makes clear personal email should be through a separate account
- provides highly restricted simulated environments for email with children
- does not publish personal email addresses of pupils or staff on the school website. Anonymous or group email addresses are used, for example office@brooklandinfant.barnetmail.net for communication with the wider public
- will contact the Police if one of our staff or child receives an e-mail that we consider is particularly disturbing or breaks the law.
- will ensure that email accounts are maintained and up to date

- uses a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Children:

- children are taught about the function of email and during their computing lessons in KS1 they explore the sending and receiving of email through an email simulation on Purple Mash.
- children do not have access to personal emails at school.
- use the LGfL pupil email addresses, when required, which are intentionally 'anonymised' for pupil protection

Staff:

- only use the LA or LGfL e mail systems on the school system
- use LA or LGfL e-mail systems for professional purposes - access in school to external personal e mail accounts may be blocked
- use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption. All devices used by staff with secure data (laptops) are encrypted.

4.5 School website

- the Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- the school website complies with statutory DFE requirements
- most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs published on the web do not have full names attached. We do not use children's names when saving images in the file names or in the tags when publishing to the school website.

4.6 Social networking

We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner even there are no official/active school social media accounts.

Staff, Volunteers and Contractors:

- are instructed to always keep professional and private communication separate
- are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Arbor is the official electronic communication channel between parents and the school.

School staff will ensure that in private use:

- no reference is made in social media to students/children, parents/carers or school staff
- ensure they are not online friends with any child/student or current parents/carers. Any exceptions must be approved by the Headteacher
- ensure they do not engage in online discussion on personal matters relating to members of the school community
- ensure that personal opinions are not attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute
- ensure security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Children:

- are taught about acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- children are required to sign and follow our Home-School Acceptable Use Agreement.

Parents/carers:

- parents and carers are reminded about social networking risks and protocols through our Home School Acceptable Use Agreement and additional communications materials when required
- are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

4.7 CCTV

- CCTV in the school as part of our site surveillance for staff and child/parent safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission. Recordings are kept for 7 days. Please see the CCTV Policy for more information.

5. Data security: Management Information System access and Data transfer

5.1 Strategic and operational practices

At this school:

- the Headteacher is the Senior Information Risk Officer (SIRO)
- staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are and the information and information asset owners are listed
- staff know how to report any incidents where data protection may have been compromised
- all staff, governors and volunteers in regulated activities are DBS checked and records are held in one central record.

5.2 Technical Solutions

At this school:

- staff have secure area(s) on the network to store sensitive files
- staff are required to log-out of systems when leaving their computer and also enforce lock-out after a 30 minutes idle time
- staff use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content
- all servers are in lockable locations and managed by DBS-checked staff

- details of all school-owned hardware will be recorded in a hardware inventory
- details of all school-owned software will be recorded in a software inventory
- disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website
- where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- we use secure file deletion software.

6. Equipment and Digital Content

6.1 Mobile devices (mobile phones, tablets and other mobile devices)

- mobile devices brought into school are entirely at the owner's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- staff mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day
- the site manager and assistant caretakers phone can be on and answered in and around school site
- all visitors are requested to keep their phones on silent and must not be answered in front of children
- no images or videos should be taken on mobile devices without the prior consent of the person or people concerned
- the recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary
- the school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- school mobile phones will be taken on school trips. Staff's personal mobile devices will only be used during school trips with permission from the Headteacher or EVC.

6.2 Use of personal devices

Staff:

- staff may use their phones during break times in a designated area, e.g. the staffroom or preferably one of the school offices. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times
- staff should not use their own mobile phones or device for contacting children or their families within or outside of the setting in a professional capacity unless in unprecedented circumstances, such as a National Lockdown
- in an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Safeguarding Officer

- staff must not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of children and will only use school-provided equipment for this purpose
- staff will use a school landline phone where contact with children, parents or carers is required
- if a member of staff breaches the school policy then disciplinary action may be taken.

Children:

- children must not bring mobile devices/ Smart devices such as Smart watches into school from home
- if any devices are brought into school, children's mobile devices will be handed to the Headteacher and kept securely until the end of the day and handed back directly to the parents/carers.

6.3 Digital images and video

At this school:

- we obtain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement forms when their daughter/son joins the school.
- uploading of information to the school website is restricted to SLT, the Chair of Governors, the computing coordinator and the school technician.
- we do not identify children in online photographic materials or include the full names of children in the credits of any published school produced video materials/DVDs
- staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of children
- If specific child's photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications the school will obtain individual parental or child permission for its long-term use
- access to social networking sites or newsgroups are blocked/filtered unless there is a specific approved educational purpose
- children are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- children are advised to be very careful about placing any personal photos on any 'social' online network spaces. They are taught to understand the need to maintain privacy settings so as not to make personal information public
- children are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Physical Security of equipment:

- staff to ensure laptops are kept safe from theft
- iPads to remain in locked trolleys in either the PPA room or Y2 resource room
- Staff are responsible for ensuring that doors to the PPA room and Y2 resource room are closed. At the end of the school day staff are responsible for shutting down consoles.

7. Online Bullying

7.1 Legal background

- Online-bullying is generally criminal in character. The law applies to online space.
- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

7.2 Definition

- Online bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself
- By online bullying, we mean bullying by electronic media such as:
    - Bullying by texts or messages or calls on mobile phones
    - The use of mobile phone cameras to cause distress, fear or humiliation
    - Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
    - Using e-mail to message others
    - Hijacking/cloning e-mail accounts
    - Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Instagram, Youtube, Whatsapp and Ratemyteacher.

At this school:

- we educate children both in the proper use of telecommunications and about the serious consequences of online-bullying and will, through SMSC and in Computing/ PSHE lessons and assemblies, continue to inform and educate the children in these fast changing areas
- we train our staff to respond effectively to reports of online-bullying or harassment and has systems in place to respond to it. The school endeavours to block access to inappropriate websites, using firewalls, antivirus protection and filtering systems and no child is allowed to work on the internet in any location within the school without a member of staff present
- whilst education and guidance remain at the heart of what we do, the school reserves the right to take action against those who take part in online-bullying.
- all bullying is damaging but online-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts
- the school will support victims and, when necessary, will work with the Police to detect those involved in criminal acts
- Brookland Infant and Nursery School will use, as appropriate, the full range of sanctions to correct, punish or remove children who bully fellow children or harass staff in this way, both in and out of school
- all members of the school community are aware they have a duty to bring to the attention of the Headteacher any example of online-bullying or harassment that they know about or suspect

7.3 Guidance

Staff:

- If you suspect or are told about an online-bullying incident, follow the protocol outlined below:

Mobile Phones:

- ask the child to show you the mobile phone
- note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- make a transcript of a spoken message, again record date, times and names
- tell the child to save the message/image
- go with the child and see the Headteacher or a member of SLT

Computers:

- ask the child to get up on-screen the material in question
- ask the child to save the material
- print the offending material straight away
- make sure you have got all pages in the right order and that there are no omissions
- accompany the child, taking the offending material, to the Headteacher
- normal procedures to interview children and to take statements will then be followed. Child protection procedures will be followed if necessary.

Children:

- if you believe you or someone else is the victim of online-bullying, you must speak to an adult as soon as possible. This person could be a parent/carer, your teacher, or the Headteacher
- do not answer abusive messages but log and report them
- do not delete anything until it has been shown to your teacher, parents/carer or Headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of online-bullying)
- do not give out personal details
- never reply to someone you do not know
- Parents/carers:
- it is vital that parents and the school work together to ensure that all children are aware of the serious consequences of getting involved in anything that might be seen to be online-bullying. Brookland Infant and Nursery School informs parents of the online-bullying policy and the procedures in place to deal with online-bullying.
- parents can help by making sure their child understands the school's policy and, above all, how seriously Brookland Infant and Nursery School takes incidents of online bullying
- parents should also explain to their child/ren legal issues relating to online bullying
- if parents believe their child is the victim of online bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything
- parents must contact the Headteacher immediately. A meeting can then be arranged with the Headteacher, which may involve other relevant members of staff
- if the incident falls in the holidays Brookland Infant School reserves the right to take action against bullying perpetrated outside the school which spills over into the school.

8. Prevent Duty (see safeguarding policy and Prevent: Radicalisation and Extremism appendix)

- Brookland Infant and Nursery School has become increasingly aware that the internet can be a source of potential danger as well as a valuable educational tool. The school acknowledges the role that social media can play in exposing children and young people to extremist ideologies that can contribute to the radicalisation process. Staff have undergone Prevent training and are regularly updated annually on best practice in this area. Staff have been made aware to be vigilant of children accessing online material out of curiosity and those who, perhaps displaying other warning signs, are further along the radicalisation route and to follow our safeguarding and child protection policy if there are any concerns
- our network filtering system, hosted by the LGFL, is configured to deal with extremist internet traffic. We are aware that extremist organisations will use the so-called 'dark net' and those seeking to access online materials will explore ways of subverting filtering systems such as using Virtual Private Networks (VPNs)
- staff are trained to be vigilant in identifying and responding to potential incidents of extremism and radicalisation and report any incidents or concerns to the designated child protection team
- children are actively taught British Values as part of our Brookland Values (see SMSC policy and provision map). Children are taught to be discerning and critical users of the internet both in school and at home
- we are currently exploring ways in which the computing curriculum can be part of a wider whole school curriculum for combatting extremist ideology by promoting fundamental British values. Computing lessons will continue to ensure that its provision for Social, Moral, Spiritual and Cultural (SMSC) education encompasses British values.

9. Related policies

- Equality Policy
- PSHE Policy
- SEN and Inclusion Policy
- Computing Policy
- Blended Learning Policy
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Management Policy
- Health and Safety Policy
- Personal, Social and Health Education Policy
- CCTV Policy.

10. Additional Information – refer to:

- Acceptable Use Policy for staff
- Home – School Acceptable Use Agreement
- KCSiE 2025