Gillespie Primary School



Online Safety Policy

October 2026

Contents

1. Introduction and Overview
    - Rationale and Scope
    - How the policy is communicated to staff/pupils/community
    - Roles and responsibilities
    - Reviewing and Monitoring
2. Education and Curriculum
    - Pupil online safety curriculum
    - Staff and governor training
    - Parent awareness and training
    - Online safety information in School
3. Expected Conduct and Incident Management
    - Expected Conduct
    - Main Areas of Risk
    - Handling Incidents
4. Managing the IT Infrastructure
    - Internet access, security (virus protection) and filtering
    - Network management (user access, backup, curriculum and admin)
    - Passwords policy
    - E-mail
    - School website
    - Learning platform
    - Social networking
5. Data Security
    - Management Information System access
    - Data transfer
    - Asset Disposal
6. Equipment and Digital Content
    - Personal mobile phones and devices
    - Digital images and video

Appendices

A1: SMART Poster

A2: Acceptable Use Agreement -Pupils EYFS and KS1

A3: Acceptable Use Agreements – Pupils KS2

A4: Acceptable Use Agreement- Staff and volunteers

A5: Parent photo/video permission form

A6: On-Line Safety Incident Report Form

A7: Additional guidance and information

1. Introduction and Overview

This policy applies to all members of Gillespie Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of Gillespie Primary School. The policy should be read in conjunction with our Child Protection Policy and Staff Code of Conduct.

The policy takes account of Government legislation and guidance for the safe and secure provision of on-line education in school and remote education in the event of whole school Lockdown or individual classes or children sent home to self-isolate.

The DSL has overall responsibility for on-line safety and liaises with our ICT provider, staff, governors and our data protection officer to ensure it is effectively managed and monitored

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

• 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

The school will carry out an annual review/audit to self –assess against the filtering and monitoring standards. This will be done in conjunction with RA technologies, our ICT provider. The head will review checks made on the schools filtering and monitoring systems and report to the Chair of the governing Board Safeguarding committee or Governing Board.

All staff know about their role and responsibilities in relation to filtering and monitoring systems on the school IT network and on school devices, including using the reporting system to inform our IT provider and the DSL if they identify a concern in relation to inappropriate or harmful material being accessed in school.

The school can additionally use the DFE's 'plan for technology for your school service' *to* self –assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them and 'Generative AI: product safety expectations to support schools to use generative artificial intelligence safely.

The policy takes account of guidance in keeping children safe in education September 2026 on: Online safety and the awareness of the four areas of categorised risks (the 4 C's)

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

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subject to harmful online interaction with other users or generative AI applications that simulate this; for example: peer on peer abuse, commercial advertising and adults posing as young children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** online behaviour that increases the likelihood of, or causes harm; for example, making, sending and receiving explicit images including those generated by AI and online bullying; and
- **Commerce-**risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The purpose of this policy is to:

- Safeguard and protect the children and staff.
- Set out the key principles expected of all members of the school community at Gillespie Primary School, with respect to the use of IT-based technologies.
- Assist school staff to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with the school's anti-bullying and child protection 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.

Communication:

The policy is communicated to staff, pupils, parents, volunteers and visitors in the following ways:

- Policy is posted on the school website and in the staffroom.
- Policy is 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 pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Reviewing and Monitoring Online Safety

- The online safety policy is referenced within other school policies including Child Protection policy, Anti-Bullying policy, Acceptable Use Policy and Data Protection Policy.
- The online safety policy will be reviewed every two years 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. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.
- The school and Network Manager R.A Technologies will take appropriate measures to ensure the school meets the cyber security standards for schools and colleges

The school will monitor the impact of the policy using:

- Logs of reported incidents
- LGFL filtering and monitoring logs of internet activity
- Surveys of parents/ carers, pupils and staff

DFE 'Teaching online safety in schools.

https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

'This non-statutory guidance outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It complements existing subjects including:

- *Relationships Education*
- *Health Education*
- *PSHE*
- *Computing'*

The guidance focuses on '*the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently*'

The teaching will be:

- Built into existing lessons across the curriculum – including Purple Mash Computing Scheme and the Islington PSHE Scheme
- Covered in specific on-line safety lessons
- Covered using school –wide approaches i.e. Anti-bullying week, Internet Safety week, Healthy living week.

Remote Education

Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and providing remote education: guidance for schools - GOV.UK (www.gov.uk).

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Takes overall responsibility for online safety provision • Is adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • Leads a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • Takes overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice. • Ensures the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • Is responsible for ensuring that all staff receive suitable online safety training • Ensures suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • Ensures Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • Ensure school website includes relevant online safety information. • Ensure that the school continues implementing its mobile phone policy which maintains that the school is a mobile free environment for all children. From Sept 2026 this is a statutory requirement. - at parental request Y6 pupils may leave their mobile phones at the school office for collection when school is over.
Designated Safeguarding leads Mark Owen & Lyn Jones	• Take day to day responsibility for online safety issues • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • Communicate regularly with Senior Leadership Team and the designated Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs • 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

Role	Key Responsibilities
	• Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Are regularly updated in online safety issues and legislation, and are aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• Ensure that the school has in place policies and practices to keep the children and staff safe online • Approve the Online Safety Policy and review the effectiveness of the policy • Support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Curriculum Leader	• Oversees the delivery of the online safety element of the Computing curriculum
Network Manager/technician- our providers are RA Technologies	• Reports online safety related issues to the Designated Safeguarding Officers • Manages the school's computer systems, ensuring - school password is kept confidential - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • Keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • Checks that school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher – from Sept 2026 this includes supporting the school to carry out an annual review /self-assess against the schools filtering and monitoring systems • Keeps up-to-date documentation of the school's online security and technical procedures
Data Protection Officer	• Responsibility for data protection compliance
Business Manager	• Ensures that the data they manage is accurate and up-to-date

Role	Key Responsibilities
	• Reports data related safety issues that come to their attention, to the Designated Safeguarding Officers and the Data Protection Officer • Ensures best practice in information management. I.e. has appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • Ensures the school is registered with Information Commissioner
LGfL Nominated contact(s)	• Ensures all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• Embed online safety in the curriculum • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
All staff, volunteers and contractors.	• Read, understand, sign and adhere to the school staff Acceptable Use Policy, and understand any updates annually. The AUP is signed by new staff on induction. • Report any suspected misuse or problem to the data protection officer • 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 **Exit strategy** • At the end of the period of employment or volunteering return any equipment or devices loaned by the school. This includes 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.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • 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 • Understand the importance of adopting safe behaviours and 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

Role	Key Responsibilities
	• Contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• Read, understand and promote the school's Pupil Acceptable Use Policy with their children • Consult the school if they have any concerns about their children's use of technology • Support the school in promoting online safety through the Home –School Agreement: 'Ensure ***my child follows the school Acceptable Use Policy and ensure they are being safe when using technologies at home 'and*** through the parent photo & video permission form agree the school's use of photographic and video images for their child.
External groups including Parent groups	• Any external individual/organisation must sign an 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.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Supports children and families to use key online platforms and tools safely including, Google Classroom, Google meet and Purple Mash consistently throughout the school;
- Reminds pupils about their responsibilities through the pupil Acceptable Use Policy;

- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;

Staff Training

This school:

- makes regular training available to staff 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.

Parent awareness and training

The school provides guidance for parents and carers about online safety including informing parents about what activities their children are being asked to do online at school and the sites they will be asked to access. Teachers will inform parents if and when their children going to be interacting with anyone online as part of their learning.

On-line safety information in school:

- The computer suite and classrooms contain posters about on-line -safety. On-line Safety is taught through the newly revised Islington Computing curriculum and through some PSHE lessons. The school holds yearly E-safety events either in Internet safety week or on Safer Internet Day.
- All staff are given a copy of the on-line -safety policy and its application and importance explained. The policy is made available for supply teachers. All staff are asked to sign an acceptable use policy. Training on e-safety is provided.
- Parents can access the Acceptable Use Policies on the school website. They are asked to read this with their children and to try and ensure the same ideas for safety are being used at home. They are updated on e-safety issues at least once a year (on Safer Internet Day or E-safety week)

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to immediately 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 in and out of school;
- know and understand school policies on the use of mobile and hand-held devices including cameras;
- store all personal data in lockable storage cabinets or a lockable storage area.

Staff and volunteers

- Known to be vigilant in the supervision of children at all times, and have control over online learning resources when children are working on computers.
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils

Parents/Carers

- Provide consent for pupils to use the Internet, as well as other technologies, as part of the school's admission form and support the school's on-line safety acceptable use agreement form;
- Know and understand what the school's rules of appropriate use for the whole school community' are and what sanctions result from misuse.
- Are provided with information and material via the website, and where possible, through relevant training to support their children in the safe use of key online platforms including Google Classroom and Purple mash when remote learning.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Designated Safeguarding Officer acts as first point of contact for any incident along with the Data Protection Officer.
- Any suspected online risk or infringement is reported to the Designated Safeguarding Officer and the Data Protection Officer.
- 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, the LADO (Local Authority's Designated Officer) and the DPO (Data Protection Officer).
- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- all members of the school are encouraged to be vigilant in reporting issues, in the confidence they 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 issues;
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that has serious safeguarding implications or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use could be monitored by the Head if an issue arises which requires investigation;
- has filtered secure broadband connectivity through the LGfL and uses it to block inappropriate sites e.g. adult content, race hate, and gaming. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses Universal Sign On (USO) user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus and Malware Bytes Anti-Malware software (from LGfL);
- Uses DfE, LA and LGfL approved systems including, secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Does not allow staff to access 'protect-level' (sensitive personal) online 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.

Network management (user access, backup)

Gillespie School

- 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;

- 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);
- Storage of all data within the school will conform to the EU and UK data protection requirements.

To ensure the network is used safely, the school:

- Ensures staff read and sign that they have understood the school's online safety Policy. This applies to their 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 different/use the same username and password for access to our school's network.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils 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 clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies;
  e.g. Borough email or Intranet; 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 and LA secure systems for all Common Transfer Files sent to other schools;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which no longer need to be stored.

Password policy

- This school makes it clear that staff must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff using critical systems to use two-factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, London Staff mail and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses.
- Will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Ensures that email accounts are maintained and up to date
- Uses LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff:

- Staff will use LA or LGfL e-mail systems for professional purposes
- 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.

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 web site 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;

- The school is in process of reviewing and updating the website and will be removing photos of children as part of this process by the end of 2026. This in response to the risk posed by AI artificially generated images using real photos.

Social networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate.
- Teachers 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.
- The use of any school approved social networking will adhere to the staff protocol, code of conduct and data protection legislation.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be on-line friends with any pupil.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our age-appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental 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.

- Parents are advised not to comment on other children or parents on their own social network sites.

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

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact are for key school information are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to lock their desktop when leaving their computer.
- Paper based sensitive information is either shredded using a cross-cut shredder or collected and stored in a lockable storage area to be bulk shredded by a company who complies with the GDPR and provides a certificate of destruction.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to the LGfL content.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE/other schools.
- 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

6. Equipment and Digital Content

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

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Older pupils (Y6) are allowed to bring mobile devices into school only on request by parents and with the school's express consent. Phones must be turned off (not placed on silent) and stored in the school office on arrival at school. They must remain turned off and in the school office until the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, or their families within or outside school. Personal phones cannot be used during lessons or formal school time. However, staff may use their own phone to contact the school when off-site with pupils i.e. when on a class trip.
- The Bluetooth or similar function of a mobile device should be switched off at all times when in school.
- Staff members may use their phones during school break times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All visitors are requested to keep their phones on silent.
- 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.
- Staff visitors and volunteers should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Digital images and video

In this school

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- By the end of the school year 2026/27 no identifiable photography of pupils will appear in on-line materials including on the school website
- 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 pupils;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

- Pupils 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;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- By the end of KS2 children are taught about the basic principles of copyright and how it could impact upon their actions.

Sexting / Nude Selfies / Live streaming:

Children do not have use of mobile phones during school time. However, if the school learns of any sexting or other inappropriate use of online devices involving one of our pupils, we will work with parents and any other appropriate authorities following procedures specified in our Child Protection Policy

As part of online safety education and the PSHE curriculum, year 5 and 6 pupils will be taught about the dangers of sexting, taking nude selfie photographs or live streaming that allows for engagement with known or unknown parties.

APPENDICES

A1 SMART Poster



Gillespie Primary School

EYFS & KS1 Acceptable Use Policy

Think before you click!!

Are you being?

 Safe	**I will only use the internet and email with an adult.**
 Always	**Click on icons and links when I know they are safe or when my teacher has asked me to.**
 Friendly	**I will only send friendly and polite messages and will only send them to people I know and trust.**
Every time	I see something I don't like on screen; I will always tell an adult straight away.

Year ___

We agree to follow these rules, signed....

Gillespie Primary School

KS2 Acceptable Use Policy

When using the computers in school I will.....



- follow the SMART rules
- always follow my teacher's instructions
- only visit websites which my teacher has recommended
- always keep my passwords and personal details a secret
- make sure all messages'/blogs/ comments I make and send are respectful
- only email people I know or those approved by a responsible adult
- never pass on anyone's email address or details without their permission
- tell a responsible adult straight away if I see **anything** I am unhappy with or receive a message I do not like

I understand these rules are there to help keep me safe. I agree to follow them and understand what the consequences will be if I do not.

Year ____ agree to these rules.

Signed....

Gillespie Primary School
Staff Acceptable Use Policy

To ensure all staff at Gillespie are aware of their professional responsibilities when using digital technology i.e. e-mail, internet, social media and network resources. They must read and sign the following Acceptable use policy. (For further information and clarification on these matters, please consult the school's on-line safety policy)

- I agree to use the internet appropriately and only for professional purposes.
- I will not use social networking sites during school hours
- I will endeavour to keep all passwords and personal information safe and confidential
- I will only use my school email account for professional purposes
- I will only access school resources remotely (such as from home) using the *LGfL/school approved system* and follow e-security protocols to interact with them
- I will follow the school's on–line Safety Policy on use of mobile phones
- I will only use school approved equipment for taking photographs/videos and for any storage, editing or transfer of digital images/videos and only save photographs on the school network drive.
- I will promote on-line safety with the children as part of teaching the computing curriculum in my class and try to ensure that they develop a responsible attitude towards digital technology
- I agree to follow school data security protocols. Confidential data must be protected by encryption and can only be transported from one location to another via the office and with approval of the Headteacher.

Signed……

Date……..

A5: Parent Photo and Video Permission form

We would like your consent to take photos/videos of your child, and use them in the ways described below. Please note that for safeguarding purposes we take a photo of your child for our school's Management Information System.

As part of our school activities and events, we may take photographs and record images of individuals within our school. The use of school photographs includes notice boards, displays, Google classroom and in school newsletters. Any other use of images including online would require separate permissions sought where necessary.

Staff taking and using photographs and videos of children will adhere to this policy and related documents, including but not limited to:

- Safeguarding and child protection policy
- Online safety policy
- Acceptable use agreement

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. You can withdraw consent by emailing office@gillespie.islington.sch.uk

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos. This can be found on our school website.

I give permission for my child's photo/video to be used as described above			Yes / No
Signature of Person with Parental Responsibility:		**Date:**	

A6 On-line safety incident Report Form

On-line safety Incident Report Form

Date	**Where incident occurred**
Type of incident? **Safety concern** ☐ **Misconduct** ☐	
What happened? (describe below)	
Actions taken?	
Any further action required?	

A7: Additional information and guidance

More information can be found in paragraphs 164-177 of keeping children safe in education 2026:

DfE advice for schools: teaching online safety in schools

UK Council for Internet Safety (UKCIS) 37 guidance: Education for a connected world

UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

The UKCIS external visitor's guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors

National Crime Agency's CEOP education programme: Thinkuknow

Public Health England38: Every Mind Matters

Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

LGFL 'Undressed' provides schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders.