Deansbrook Infant School

Online Safety Policy

Reviewed and ratified by the Governing Body: November 2022

Review Date: November 2024

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Deansbrook Infant School with respect to the use of IT-based technologies
- Safeguard and protect the children and staff at Deansbrook Infant 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 pupils.

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

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)

Development/Monitoring/Review of this Policy

This online safety policy has been developed by:

- Headteacher: Carole Catley
- Online Safety Officer: Nikki Simon
- Staff – including teachers, support staff, technical staff
- Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by Governing Body on	November 2022
The implementation of this online safety policy will be monitored by	Nikki Simon: Online safety officer
The online safety policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2024
Should serious online safety incidents take place, the following external persons/agencies will be informed	LADO, Police where appropriate

The school will monitor the impact of the policy using:

- Monitoring logs of internet activity (including sites visited)/filtering)
- Internal monitoring data for network activity

Scope of the Policy

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

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The Online Safety Governor is Ryan Hannan.

The role of the Online Safety Governor will include:

- meetings with the Online Safety officer
- monitoring of online safety incident logs
- reporting to relevant Governors Committee

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents appendix 1)
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety officer

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority if needed
- Liaises with school technical staff
- Reports regularly to the Senior Leadership Team

Network Manager/Technical staff –

- Those with technical responsibilities are responsible for ensuring:
- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority/ relevant body online safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the *networks/internet/digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Lead for investigation/action/sanction

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the staff acceptable use agreement (AUA)
- They report any suspected misuse or problem to the Headteacher/ Online Safety Lead for investigation
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems eg teachers2parents/Tapestry/Google Classroom
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Officer

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

Pupils

- Are responsible for using the *school* digital technology systems in accordance with the pupil acceptable use agreement
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies both in and out of school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice. They will:

- Support their children to keep safe when using the internet at home. If advice is required to do this they may contact the online safety officer.
- Ensure that any digital and video images taken at school events will not be shared on social media. All parents will sign a declaration stating this when their child starts at Deansbrook infant school.

Education and curriculum

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites). Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The

online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. A planned online safety curriculum should be provided as part of computing lessons and should be regularly revisited. Key online safety messages should also be reinforced as part of a planned programme of assemblies.

Pupils will be taught to:

- Understand the importance of using 'strong and safe' passwords
- STOP and THINK before they CLICK
- 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
- Understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- Understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
- 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 how to ensure they have turned-on privacy settings
- Understand why they must not post pictures or videos of others without their permission
- Understand the impact of cyberbullying, know how to seek help if they are affected by any form of online bullying
- 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 button
- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Technical – infrastructure/equipment, filtering and monitoring

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."

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

- School systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Users will be provided with a username and secure password
- Users are responsible for the security of their username and password. I
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Email

Staff at this school use the StaffMail system for all school emails. This system is linked to the USO authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents/carers, as well as to support data protection. General principles for email use are as follows:

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL. Internally. If personal data does need to be shared by email, information should be password protected using a strong password and the email address verified before sending to prevent a data breach.
- Staff should use the school network or the Google Drive, including when working from home when remote access is available.
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination. See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher is responsible for ensuring that the website content is accurate and complies with DfE requirements. Day-to-day responsibility of updating the content of the website to is delegated to a member of staff. Where other staff submit information for the website, they are asked to remember:

- Schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.
- Where pupil work is published on the website, the identities of the pupils are protected unless specific consent has been obtained

Google Drive

Deansbrook Infant school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. The data protection officer and technical support analyse and document systems and procedures before they are implemented, and regularly review them. The following principles apply

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication for access to staff or pupil data will be used when possible and as it can be implemented in to school systems.
- Only school-approved platforms are used by staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

Staff, pupils' and parents/carers' social media presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents/carers, staff and pupils will use it. However, as stated in the acceptable use agreements which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups. If parents/carers have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents/carers, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media. All members of the school

community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video) and permission is sought before uploading photographs, videos or any other information about other people.

Personal devices including wearable technology and bring your own device (BYOD)

- Mobile phones brought into school are entirely at the staff member, and parents/carers' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff must not use mobile phones to take pictures or videos of children in any circumstances.
- Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school.
- Staff should not share their personal mobile phone numbers with parents/carers. Parents/carers who accompany a school trip should be given the main school phone number for contact purposes.
- Child/staff data should never be downloaded onto a private phone.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents/carers, 14 they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Parents/carers are asked to leave their phones in their pockets and turned off when they are on site.
- Visitors/Contractors are not permitted to use mobile phones and or any other devices use anywhere in school, around the children.

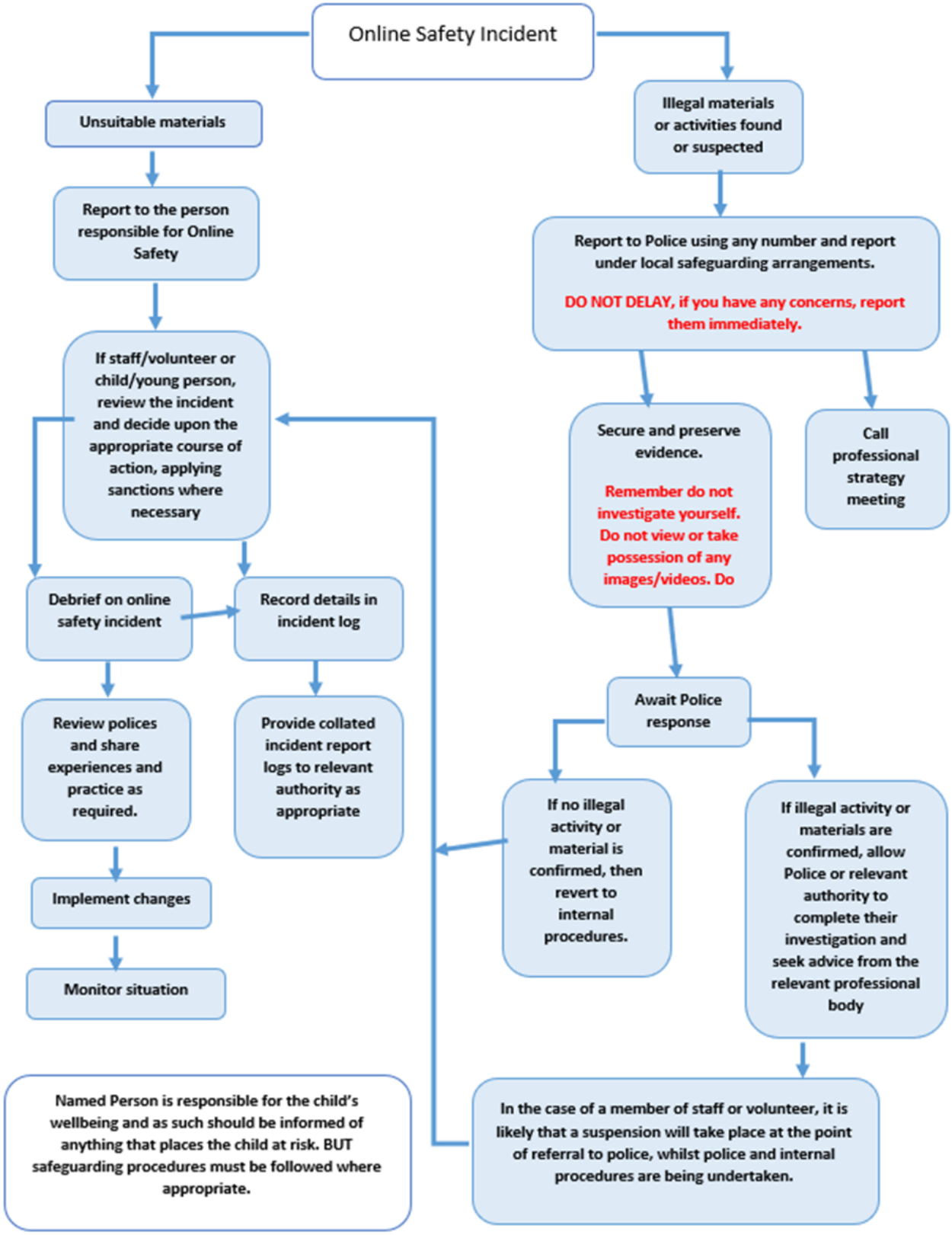
Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant equipment that may have held personal data will have the storage media forensically wiped or destroyed by an authorised company. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. 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

Related policies:

- Safeguarding and Child Protection Policy
- Mobile phone policy
- GDPR policy
- Anti-Bullying Policy
- Relationships and Behaviour Policy
- Data Protection Policy

Appendix 1


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.