E-Safety Policy

Last review date:	**24/01/24**
Approved by:	**Governing Body on 30/01/24**
Next review date:	**24/01/26**
Person/s responsible:	**Mrs F.Ghosseiri – Assistant Head**

E-Safety Policy

Table of Contents

1. **Introduction**

At Danegrove Primary School, we believe in preparing our pupils for the rigor and expectations of the current world, which includes the ever-changing connectivity to people through the Internet and social media.

E Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Why Is Internet Use Important?
The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Danegrove Primary School has a duty to provide pupils with quality internet access allowing them to learn how to access, analyse and evaluate the online information and to take care of their own safety and security.

Benefits of using the internet in education include:

- access to world-wide educational resources including museums, libraries and art galleries
- rapid and cost effective worldwide communication
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management
- networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority
- access to learning wherever and whenever convenient
- greatly increased skills in Literacy
- in times of home learning, internet access allows teachers to teach remotely and pupils to continue learning remotely

2. Aims

At Danegrove Primary School**,** we understand the responsibility to protect and educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We aim to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors and to establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Both this policy and the ICT Policy (for all staff, governors, visitors and volunteers) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, interactive smartboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets, mobile/smart phones, and portable media players, etc).

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be:

- to confirm or obtain School business related information;
- to confirm or investigate compliance with School policies, standards and procedures
- to ensure the effective operation of School ICT
- for quality control or training purposes
- to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of School IT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the E-Safety Co-ordinator or the Head teacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head teacher.

3. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education September 2023, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

4. Implementation and Computer Viruses

All files downloaded from the Internet, received via email or on removable media (e.g. connected phones/tablets, USBs) must be checked for any viruses using school provided anti-virus software before using them. Never interfere with any anti-virus software installed on school IT equipment that you use. If a machine is not routinely connected to the school network, provision must be made for regular virus updates through the IT support provider.

If anyone suspects there may be a virus on any school IT equipment, they stop using the equipment and contact the IT support provider immediately. The IT support provider will advise what actions to be taken and is responsible for advising others that need to know.

5. E-Safety Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in this school is the IT lead who reports directly to the Head teacher.

6. **The Governing Body**

The Governing Body has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation. The governing board will meet with the E-Safety Coordinator/designated safeguarding lead (DSL) to discuss online safety.

The governor who oversees online safety is Emily Armer (Safeguarding Governor).

All governors will:

- ensure that they have read and understand this policy
- agree and adhere to the terms on the IT Usage Policy and the Social Media Policy

7. The Head teacher

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

8. The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding and child protection policy. The DSL takes lead responsibility for online safety in school, in particular:

- supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the head teacher, contracted engineer and other staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- updating and delivering staff training on online safety
- liaising with other agencies and/or external services if necessary

9. The Contracted School Engineer

The engineer is responsible for:

- working with London Grid for Learning (LGFL) to put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting a full security check and monitoring the school's IT systems on a weekly basis
- working with LGFL to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ensuring that any online safety incidents are logged with the DSL and dealt with appropriately in line with this policy

10. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- working with the DSL to ensure that any online safety incidents are logged

11. Parents

We believe that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of school and also to be aware of their responsibilities. We consult and discuss on E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to IT and associated risks. Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents/carers are required to make a decision as to whether they consent to images of their child and themselves being taken/used in the public domain (e.g., on school website, newsletters etc.).

The school disseminates information to parents relating to E-Safety where appropriate in the form of

- parent coffee mornings
- External talks, for example Prevent
- NSPCC lead online safety information sessions
- posters/flyers
- website postings
- newsletter items
- digital parenting magazine

Parents are expected to:

- notify a member of staff or the Head teacher of any concerns or queries regarding this policy
- ensure their child has read, understood and agreed to the terms on the acceptable use & E-safety agreement.

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Home Activity Packs - Thinkuknow.co.uk: https://www.thinkuknow.co.uk/parents/home-activity-worksheets/

12. Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

13. Educating Pupils about E-Safety

IT and online resources are regularly used across the curriculum. We believe it essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum. Pupils will be taught about online safety as part of the curriculum.

Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or organisations such as Childline.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community. New staff receives information on the school's acceptable use policy and social media policy as part of their induction, alongside the information contained in the Pupil's Acceptable Use & E-Safety Agreement. We endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

14. Managing Other Technologies

Technologies including social networking sites, (if used responsibly both outside and within an educational context), can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavours to deny access to social networking sites to pupils within school. All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are. Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests).

15. Remote Learning

In the event that remote learning has to take place, whether that be for an individual child isolating, a bubble/year group isolating or in event of a national lockdown then the school will implement the school's Contingency Plan for Online teaching.

Remote learning at Danegrove Primary School will ensure that we stay connected with the school community by both allowing us to continue the learning process and by providing support for pupils' wellbeing.

The platform that will be used for all remote learning sessions are ~~Seesaw and~~ Google Classrooms where we will use a blend of live teaching and pre-recorded lessons alongside lessons via Oak Academy. Details about each remote learning session and any additional resources will be posted ~~via Seesaw~~ Google Classroom.

Danegrove Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school website will contain information and links to support both parents and children with the appropriate resources to keep safe whilst learning online.

15.1. Devices

Any device that is provided by the school for the purposes of remote learning will have suitable anti-virus and safeguarding software installed, can establish secure connections and allows for audio and visual material to be recorded or downloaded, where required.

Any device that is loaned by the school will be accompanied by a school/parent signed Long Term (or Short Term) Equipment Loan Agreement.

15.2. Communication

Teachers will be permitted to communicate with parents and pupils via phone or sometimes video call if the school is in partial or full lockdown, if face to face contact is restricted or they are having to teach remotely. Teachers can communicate with parents and pupils at any time via the child's ~~Seesaw account~~ Google Classroom as long as the communication is in regard to school issues only.

When staff members contact children/parents by phone, email or video calling they will ensure that:

- they either use an app like 3CX that will route calls through the school's number rather than their own, or block their number so that it can't be seen.
- they only contact a child via the parent's phone and never directly to a child's phone
- they have a parent there at the child's end, and have the phone on speaker phone
- they only send a message from their ~~Seesaw~~ Google Classroom account and never from a personal account.
- they only communicate with a child via the child's ~~Seesaw~~ Google Classroom account and never to a child's personal email account.
- they communicate within school hours as much as possible
- the conversation and the language used is professional and appropriate
- the date of the phone call/video call is recorded and who was spoken to, including the parent's name
- all messages and forms of communication are kept
- any concerns are raised as soon as reasonable possible with SLT, including any concerns raised during any communication.

15.3. Pre-recorded and Live Teaching

Where teaching is being undertaken remotely the teacher will ensure that they follow the same approach as laid out in the staff code of conduct. Staff must maintain professional boundaries at all times to both protect the children in their care and ensure that the children and the teacher feel safe, respected and valued.

Danegrove Primary School is committed to keeping their pupils safe, including online. Whilst children are learning at home the school will ensure that at least one of the weekly activities set for home learning is a 'Keeping Safe Online lesson'.

To help with pupils' wellbeing there will be opportunities for 'online playtimes' to take place – these will always be supervised by the teacher or teaching assistant.

When teachers are teaching a pre-recorded lesson:

- dress like you would for school
- avoid recording any lessons with images or distractions (only a neutral background)
- use professional language at all times
- keep a record of who is accessing the learning

When teachers are teaching live lessons remotely they must:

- ensure that any live lessons take place during school hours and are supervised.
- sit against a neutral background
- avoid recording in their bedroom where possible (if that's not possible, use a neutral background)
- dress like they would for school
- double check that any other tabs they have open in their browser would be appropriate for a child to see, if they're sharing their screen
- use professional language
- where possible, ask pupils to also be in a shared space in their house, rather than in their bedroom
- ask that children are dressed appropriately and to either blur their background or apply a background
- ask parents who'll also be there to be mindful that other children might see or hear them and anything in the background
- respond to behaviour concerns as they would in the classroom
- expect to be treated with respect by any adult within the child's house and report any concerns immediately to SLT
- make a recording so there's something to go back to later on if you need to, and keep a log of who's doing video calls and when. Check that parents are happy with you making recordings first – tell them it's for school records only.
- ensure that the chat facility is supervised and monitored and is only be used for educational and/or lesson purposes – any inappropriate use of the chat facility will be shared with SLT.
- Keep a record of attendance for all live lessons.

Teachers/TAs should communicate with the Head teacher or DSL should any interactions not be appropriate or conducive to learning.

Staff who interact with children, including in live lesson, via Google Classroom Chat facility, over the phone or via Seesaw, will continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection and Safeguarding Policy and should be raised as soon as reasonable possible with the DSL and put in writing, whether that be on CPOMs or emailed directly to the DSL.

The School's Child Protection and Safeguarding Policy, ICT Policy and the Staff Code of Conduct must be adhered to at all times.

16. **Cyber-bullying**

Definition: Cyber-bullying takes place online, such as through social media, messaging apps, gaming sites and mobile phones. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

16.1. **Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils:

- understand what it is and what to do if they become aware of it happening to them or others.
- know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, IT lessons and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and the Safeguarding & Child Protection Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

17. **Publishing Pupils' Work**

On a child's entry to the school, and in accordance with GDPR, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video
- in display material that may be used in the school's communal areas
- general media e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Pupils' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Before posting pupils' work on the Internet, a check will be made to ensure that permission has been given for work to be displayed.

18. Mobile Technologies

Many emerging technologies offer further opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, iPads/tablets, gaming devices, mobile and smart phones are familiar to children outside of school, providing children with internet access and thus open up risk and misuse

associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways so that users use them appropriately:

- Pupils who are in year 6 and travel to school independently may bring a mobile/smart phone.
- The pupils place their phones into a tray which will be locked away in the classroom by their class teacher, and at the end of the day retrieve their own phone.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under normal circumstances the school does not allow a member of staff to contact a pupil or parent/carer using their personal device. However, during ~~COVID-19~~ remote learning a staff member may be working from home and may need to use a personal device to contact children/parents by phone, email or sometimes video calling. In this case they will ensure that they either use an app like 3CX that will route calls through the school's number rather than their own, or block their number so that it can't be seen.
- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Personal devices are not allowed to be used to record any image or sound of any pupil.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff are required to sign the Acceptable Use Agreement form for usage of their devices.

18.1. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the IT coordinator. Work devices must be used solely for work activities.

19. Examining Electronic Devices

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

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

- cause harm, and/or
- disrupt teaching, and/or
- break any of the school rules

If inappropriate material is found on the device, and in accordance with the Safeguarding and Child Protection Policy, it is up to the staff member **in conjunction with the DSL** or another member of the senior leadership team to decide whether they should:

- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- report it to the police

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.
Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

20. Acceptable use of the internet in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet, as per the IT Policy.

All pupils and parents are expected to sign a Pupil Acceptable Use & E-safety Agreement.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

21. **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety regularly.

Volunteers will receive appropriate training and updates, if applicable.

Links with other polices:

This E-Safety Policy is linked to our:

- Safeguarding & Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT Policy
- Social Media Policy