The Greville Primary School

On Line Safety Policy

Last update: October 2024

Governors' Committee Responsible	Learning & Teaching
Policy Originator	Duncan Steele
Next Review Date:	November 2026

Writing and reviewing the Online Safety Policy
This Online Safety Policy outlines the commitment of The Greville to safeguard members of our school community online in accordance with statutory guidance and best practice.
This Online Safety Policy applies to all members of the school community (including staff, children governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.
The Greville will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy relates to other policies including those for behaviour, safeguarding, mobile phones, staff code of conduct and anti-bullying.

- The school has an Online Safety Leader, who is also the lead DSL, and this person is Duncan Steele and he will work closely alongside the computer subject leader
- The policy has been written by the school, building on best practice and government guidance. It has been agreed by the Leadership Team and approved by governors
- The policy and its implementation will be reviewed every 2 years.

The DfE Keeping Children Safe in Education guidance suggests that:

- The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as 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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. The following section outline the online safety roles and responsibilities of individuals/groups within the school.

<u>Headteacher and senior leaders</u>

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and other members 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.
- The headteacher is responsible for ensuring that the Designated Safeguarding Lead/Online Safety Lead, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will receive monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher will work with the responsible safeguarding governor, DSL, computing

leader and and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the safeguarding governor who will receive regular information about online safety incidents and monitoring reports. This member of the governing body will:

- Have termly meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly review (anonymised) reports of online safety incidents
- Check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- Ensure that the filtering and monitoring provision is reviewed and recorded, at least annually. (in-line with the DfE Filtering and Monitoring Standards)
- Report to the full governing body on online safety

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*
> *They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"*
> *They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school has chosen the **computing subject leader** to work in support of the DSL in carrying out these responsibilities.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers (Eduthing) on matters of safety and safeguarding and welfare (including online and digital safety)

Computing subject leader

This person will work alongside the DSL in order to:

- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond, including paretns/carers
- develop a planned and co-ordinated online safety education programme e.g. ProjectEVOLVE, assemblies, Safer Internet Day
- liaise with teachers and the curriculum leader to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by children) with regard to the areas defined In Keeping Children Safe in Education: content, contact, conduct and commerce.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff code of conduct, which includes online safety expectations
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure children understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, children are 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*
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Teaching and learning

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children
- The school will provide an age-appropriate online safety curriculum with regard to the areas defined In Keeping Children Safe in Education: content, contact, conduct and commerce.
- Children will be taught to be critically aware of the materials they read

- Children will be taught how to evaluate whether a website is useful and appropriate for the task and will be taught what to do if they or another child comes across inappropriate material (See 'Rules' in Appendix B)

Managing online access and security
The school will provide managed online access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when online and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system (Senso) which is regularly checked to ensure that it is working, effective and reasonable
- The filtering system will be checked through a reporting procedure, which the Online Safety Leader (DSL) and Computing Subject Leader will monitor regularly
- If staff or children come across unsuitable on-line materials, the site must be reported to the Online Safety Leader
- Any problems arising in school should be recorded and reported to the Online Safety Leader
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by passwords
- Systems will be in place to ensure that online use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform Online safety policy.
- The security of school IT systems will be reviewed regularly.

Social Networking and Online Activity
- Children are taught not to reveal personal details about themselves or others in communication, or arrange to meet anyone without specific permission
- Staff to child email communication must only take place via a school email address and with the parents' knowledge that the e-mail exchange is taking place
- Staff do not reply to children's email unless they copy the parent in as well
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Staff and children should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. (Staff code of conduct outlines clear expectations)

Published content and the school website
- The contact details on the website should be the school address, email and telephone number
- The head teacher or any designated staff will take overall editorial responsibility and ensure that content is accurate and appropriate
- All staff will endeavour to ensure that content added to the website is appropriate and accurate, including messages to parents
- The website content will be updated and maintained by authorised individuals who will have their own identification and password in order to be able to access the site
- Images/footage of children in any media will only be used where consent has been given by parents on our 'Permission' form

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the Online safety policy and the staff code of conduct.
- Staff must not store images of pupils or pupil personal data on personal devices
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business

Using Mobile Phones and wearable devices (See more details in separate policy)

- Wearable devices, which include smart technology, are not permitted in school by children
- Only children in Years 5 and 6 may bring mobile phones in to school. Parents need to have read and signed the mobile phone consent policy.
- Mobile phones must be handed to the class teacher at the beginning of the day, where they will be stored in a safe place, and remain switched off until the end of the school day
- School cannot be held responsible for the loss of or damage to children's own mobile phones
- Responsible use of mobiles will be included in the PSHE/computing programme, including cyberbullying and appropriate use of text and photos
- As with email, children will be taught to save inappropriate messages and told not to respond; they will be encouraged to show a parent when at home or an adult when in school, if they receive anything inappropriate or offensive
- Staff will, where possible, use a school phone where contact with parents is required

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) which came into force on May 25, 2018

Internet Access and Responsibility

Authorising access

- All staff must read and sign the staff code of conduct which includes Online safety guidance
- Visitors must read and sign the 'visitor online acceptable user guide (Belinda??)
- Parents are informed that pupils will be provided with supervised internet access.
- Parents will be sent a letter which includes a copy of the **Pupil Acceptable ICT User Agreement** which their children will have read with their teachers and signed in class (Appendix B)
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the Computing subject leader and Headteacher who will investigate and take appropriate action, liaising with broadband provider if necessary
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law
- All children will have their own password to access the internet
- Online access will be supervised with filters in place

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access
- The school will monitor IT use to establish if the Online Safety Policy is adequate and that the implementation is appropriate and effective

Handling Online safety complaints/concerns

- Children should be encouraged to report any issues/concerns to parents when at home or adults in school
- KS2 children will be taught how to report concerns to Childline- the number is also visible around the school.
- If any member of staff receives a report of an issue (from a child or parent), it should be shared with the Online Safety Leader. If the staff member assesses it to be of a safeguarding nature, they should go straight to the headteacher and it will be logged on CPOMs.
- The Online Safety Leader/DSL and will consider the best course of action which will often involve contacting parents
- Children and parents will be informed of consequences for children misusing the internet
- Any complaint about staff misuse must be referred to the Headteacher
- Any complaint about misuse by the Headteacher must be referred to the Chair of Governors – contact details can be found in the Child Protection and Safeguarding Policy
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures
- For incidents which involve youth produced sexual imagery (sexting), or allegations of Child on Child abuse, please refer to the Child Protection and Safeguarding Policy.

Communication of the policy

To children

- Appropriate elements of the Online Safety Policy will be shared with children regularly
- Children will sign an Acceptable User Agreement **(Appendix A)**
- Online safety rules will be shared with the children and regular reminders will be given in lessons
- Children will be informed that network and online use will be monitored
- Rules for internet access will be posted in all classrooms
- Curriculum opportunities to gain awareness of online safety issues, and how best to deal with them, will be provided for children. This should be addressed each year as children become more mature and the nature of newer risks can be identified

To staff

- All staff, as part of their induction, should read the school's Online Safety Policy and sign the Staff code of conduct.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will either be supervised by senior management or be on the Leadership Team. They will follow clear procedures for reporting issues.
- Staff must adopt the same level of professionalism when online at home for personal use as they do at school, this includes keeping staff and children's names and details confidential
- Parents are able to contact staff and teachers on school email accounts

To Parents/Carers

- Parents will receive a copy of their child's Acceptable User Agreement
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website where there is a page on 'Online safety' with a range of useful resources and links
- The school run Online safety training for parents, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust
- Parents should be encouraged, where possible, to interact with their children on the internet as well as provide other opportunities for learning and recreation

- It is ultimately a parent's responsibility to closely monitor their child's use of technology outside of school - including use of mobile phones, the internet etc. If they have evidence of cyber-bullying involving school children and feel unable to resolve the matter themselves, they should liaise directly with the school (normally via the class teacher first) about how best to proceed

Learning & Teaching	**FGB Approval**	**Reviewed/Updated**
07.02.23	21.2.23	
15.10.24	28.11.24	

Appendices

Appendix A - Pupil Acceptable User Agreement

Greville Online Safety Rules

These rules help me to stay safe on the internet:

- I will only use the internet when there is an adult present
- I will keep personal details to myself and I will not share them with other people. E.g. my password or home address
- I will tell an adult immediately if I receive a message, or see something on the screen that makes me feel uncomfortable or upset
- I will always be polite and kind when I write and send messages
- I will only communicate with people I know or that a responsible adult has approved
- School can check my computer and be able to see what I am doing and what sites I have visited
- I will look after equipment each time I use it
- If I break these rules, I know I may be stopped from using the internet and/or using technology

Appendix B - Letter sent home to all pupils and their parents.

Dear Parents
In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At The Greville, we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. School staff should not be approached by pupils or parents online or invited to join social networks.

Your child has read the following **Acceptable User Agreement** (Greville Online Safety Rules) in class with the teacher. Once it has been fully understood, your child has signed his/her name to agree to stick by it.

Please read it again at home with your child to show your support of the school in this important aspect of our work. Thank you.

Greville Online Safety Rules

These rules help me to stay safe on the internet:

- *I will only use the internet when there is an adult present*
- *I will keep personal details to myself and I will not share them with other people. E.g. my password or home address*
- *I will tell an adult immediately if I receive a message, or see something on the screen that makes me feel uncomfortable or upset*
- *I will always be polite and kind when I write and send messages*
- *I will only communicate with people I know or that a responsible adult has approved*
- *School can check my computer and be able to see what I am doing and what sites I have visited*
- *I will look after equipment each time I use it*
- *If I break these rules, I know I may be stopped from using the internet and/or using technology*