E-safety Policy

Derwent and Southill's approach:
The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Derwent and Southill Schools with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Derwent and Southill Schools.
- 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 online bullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with children.

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

- Content
    - exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
    - lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
    - hate sites.
    - content validation: how to check authenticity and accuracy of online content.
- Contact
    - grooming.
    - online bullying in all forms.
    - identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.
- Conduct
    - privacy issues, including disclosure of personal information.
    - digital footprint and online reputation.
    - health and well-being (amount of time spent online - internet or gaming).
    - sexting (sending and receiving of personally intimate images).
    - extremism.
    - copyright.

Scope
This policy applies to all members of Derwent and Southill Schools communities (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to or are users of schools computer systems, both in and out of school. The term "Staff" covers ALL adult staff on either site, including temporary, supply and ancillary staff, and volunteers working with children. It also includes people working in before and after school clubs run by the schools as well as holiday clubs and the preschool classes (known at Southill as Martins Nursery Class).

The Education and Inspections Act 2006 empowers Executive Headteachers' to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of Derwent and / or Southill. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data.

Derwent and Southill Schools 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.

Roles and responsibilities

Role	Key Responsibilities
Executive Headteacher	● To take overall responsibility for Online Safety provision. ● To take overall responsibility for data and data security (SIRO). ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (currently E2BN and Insight ICT). ● To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant. ● To be aware of procedures to be followed in the event of a serious e-safety incident. ● To take a day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents. ● Communicate regularly with SLT and the designated Online safety Governor to discuss current issues and review incident logs. ● To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident. ● To liaise with the Local Authority and relevant agencies. ● To ensure that they are regularly updated on e-safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media
Subject leader for IT	● To ensure that Online safety education is embedded across the curriculum. ● To oversee the delivery of the online safety element of the Computing curriculum. ● To liaise with the online safety coordinator regularly.
Office manager	● To liaise with school Computing technical staff and managed service provider staff. ● To ensure that an Online safety incident log is kept up to date.
Governors / Online safety governor	● To ensure that the school follows all current Online safety advice to keep the children and staff safe. ● To approve the E-safety policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. ● To ensure that a member of the Governing Body has taken on the role of Online Safety Governor (usually the same person who is the safeguarding governor). ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities. ● To regularly review e-safety with the Executive Headteacher including Online safety incident logs.

Managed service provider (Insight ICT)	● To report any online safety related issues that arise to the Executive Headteacher. ● To ensure that provision exists for misuse detection and malicious attack (e.g. Keeping virus protection up to date). ● To ensure the security of the school IT system. ● To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • To ensure that appropriate web filtering is applied and updated on a regular basis. • To ensure that he / she keeps up to date with the school's E-safety policy and technical information in order to effectively carry out their online safety role. To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. ● To keep up-to-date documentation of the school's online security and technical procedures.

Teachers	● To embed online safety issues in all aspects of the curriculum and other school activities. ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	● To read, understand, adhere to and help promote the school's e-safety policies and guidance. ● To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices. ● To report any suspected misuse or problem to the Executive Headteacher. ● To maintain an awareness of current online safety issues and guidance (e.g. through CPD). ● To model safe, responsible and professional behaviours in their own use of technology. ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. Personal email / text / mobile phones etc.
Children	● To understand the importance of reporting abuse, misuse or access to inappropriate materials. ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-safety policy covers their actions out of school, if related to their membership of the school. ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

The curriculum

Derwent and Southill's computing curriculum…

- Has a clear, progressive online literacy framework for EYFS to Y6 including behaviours appropriate to their age and experience
- Develops in children a range of strategies to evaluate and verify information before accepting its accuracy.
- Develops in children an awareness that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- Develops in children the skills to know how to narrow down or refine a search.
- Develops in children an understanding of 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). Children MUST NEVER share passwords.
- Develops in children the ability to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- Enables children to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- Enables children to understand why they must not post pictures or videos of others without their permission.
- Enables children to have strategies for dealing with receipt of inappropriate materials.

At Derwent and Southill, staff will remind the children about their responsibilities when using ICT.

Staff and governor training

Derwent and Southill Schools…

- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Make regular training available to staff on online safety issues
- Provide, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy as enshrined in the Acceptable Use Agreement.

Parent awareness and training

Derwent and Southill Schools run a rolling programme of advice, guidance and training for parents, including ensuring that an Acceptable Use Agreements are given to all new parents to ensure that principles of online safe behaviour are made clear.

Expected Conduct and Incident management

In Derwent and Southill, all users:

- Are responsible for using the school computer systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems. (At KS1 and in EYFS, parents / carers sign on behalf of the pupils.)
- Need to understand what amounts to misuse or access to inappropriate materials and are aware of the consequences
- 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 out of school and realise that the school's E-safety policy covers their actions out of school, if related to their membership of the school.

This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private. Parents/Carers should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

In this school there is strict monitoring and application of the E-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions. All members of Derwent, Southill and their wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively by the school.

At Derwent and Southill support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues. The monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors, the Local Authority and the Local Safeguarding Children's Board.

Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible. We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

E-mail

Derwent and Southill do not publish personal email addresses of pupils or staff on the school website. We use anonymous email address for main correspondence (derwent@derwentschool.co.uk or southill@southillschool.co.uk).

We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. We will also report messages relating to or in support of illegal activities to the relevant Authority and if necessary, to the Police.

The children at Derwent and Southill are introduced to, and use, e-mail as part of the IT/Computing scheme of work through our learning platform. Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home. Specifically, they are taught:

- not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- that an e-mail is a form of publishing where the message should be clear, short and concise.
- they must not reveal private details of themselves or others in email, such as address, telephone number, etc.
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.
- that they should think carefully before sending any attachments.
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature.
- not to respond to malicious or threatening messages.
- not to delete malicious or threatening emails, but to keep them as evidence of bullying.
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.

The Executive Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. Most material is our own work but where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual email identities will not be published. Equally at Derwent and Southill photographs published on the web do not have full names attached. We also do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

The use of any social networking sites is covered in Derwent and Southill's social media policy.

Mobile phones and mobile devices:

- Mobile phones or mobile devices brought into school are entirely at the staff member, parent or visitors own risk. Derwent and Southill accept no responsibility for the loss, theft or damage of any phone or handheld device brought into school. All visitors are requested to keep their phones on silent.
- Children at Derwent and Southill are asked not to bring mobile phones or mobile devices into school. Where they do, they are handed into the office for keeping to the end of the school day. This applies to the clubs for before and after school too.
- The recording, taking and sharing of images, video and audio on any mobile phone or mobile device not owned by the school is to be avoided except where it has been explicitly agreed otherwise by the Executive Headteacher. Such authorised use is to be monitored and recorded. All mobile phone or mobile device use is to be open to scrutiny and the Executive Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. Equally no images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned as well as the consent of the Executive Headteacher.

- Derwent and Southill reserve the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents and children need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and mobile devices are not permitted to be used in certain areas within the school site such as the toilets.
- Mobile phones or mobile devices including smart watches will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity directed by a member of staff. NB: Mobile devices include tablets, ipads (of which there are some in school), i watches or any other device with the capacity to capture images or access the internet.

Students' use of personal devices

- Children at Derwent and Southill are asked not to bring mobile phones or mobile devices into school and if they do, to hand them in for safekeeping until the end of the school day. Smart watches are also to be handed in.

Staff use of personal devices

The term "Staff" covers ALL adult staff on site, including temporary, supply and ancillary staff, and volunteers working with children. It also includes people working in the before school, after school and holiday provision:

- Staff handheld devices, including mobile phones and personal cameras must not be used to take images of children. Any school files containing personal information that is downloaded onto a personal device must be deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by the Executive Headteacher in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the Executive Headteacher.
- Staff must 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.
- 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, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images - cameras and video

At Derwent and Southill:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son 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
- Staff may not use personal mobile phones / equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental permission for its use

- Children at Derwent and Southill are 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. They are also 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, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- The recording, taking and sharing of digital photographs or video on any device not owned by the school is to be avoided except where it has been explicitly agreed otherwise by the Executive Headteacher. Such authorised use is to be monitored and recorded. All devices should be open to scrutiny and the Executive Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. Equally digital photographs or video taken on any devices not owned by the school without the prior consent of the person or peole concerned as well as the consent of the Executive Headteacher.

Asset disposal

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.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. 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.

Handling complaints:

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

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include but are not limited to:

- informing parents or carers.
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework].
- fixed or permanent exclusion (in the case of children).
- formal warning or dismissal (in the case of staff).
- referral to LA / Police.

The Executive Headteacher acts as the first point of contact for any complaint. Any complaint about staff misuse must also be referred to the Executive Headteacher. Complaints related to child protection are dealt with in accordance with school / Local Authority child protection procedures.

Policy Review

The Governing Body of our school is responsible for ensuring the review of this policy, and for reporting back to the Local Authority.

Signed: Samantha Barlow (Executive Headteacher) Signed: Andrew Jackson (Chair of Governors)

Date policy reviewed: July 2025
Date of review: September 2026