E-Safety Policy

Approved: 22 May 2025 **Review: May 2026**

1. Introduction

Students interact with new technologies such as smart devices and the internet daily. These are viewed as essential elements in 21st century life. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place users in danger, so not only does the school have a duty to provide students with quality, filtered internet access as part of their learning experience but also a 'duty of care' to keep students safe by raising awareness of the risks involved and highlighting the responsibilities that accompany sensible use. We are particularly mindful of our responsibilities to raise students' awareness of 'grooming' techniques used on the internet as well as preventing access to terrorist and extremist material when accessing the internet in school and promoting resilience to radicalisation.

2. Scope of the policy

This policy forms part of the 'e-safety package' - a comprehensive set of documents and actions which relate to the safe use of the internet, mobile phones and other electronic communication technologies. This policy applies to *all* members of the school community (including staff, students, volunteers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

3. Roles and responsibilities

All users should ensure that their use is legal and ethical as well as reflecting the standards of the school community. The school reserves the right to withdraw access to any user who does not demonstrate responsible use. This section outlines the responsibilities and roles of specific individuals and groups within the school community.

3.1 Governors

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The link governor for safeguarding will oversee this area.

3.2 The Headteacher

The Headteacher is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring online safety practices are audited and evaluated.
- Working with the DSL and ICT technicians to review this policy.
- Working with the DSL and governors to update this policy on an annual basis.

3.3 The Designated Safeguarding Lead (Deputy Headteacher i/c Safeguarding)

The DSL is responsible for taking the lead responsibility for online safety in the school by:

- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Liaising with the Network Manager to review filtering and monitoring activity.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and the requirements as set out in 'Keeping Children Safe in Education' are fully implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies such as CEOP, Multi-Agency Safeguarding Hub (MASH) and/or the Police, as required.
- Keeping up to date with current research, legislation and online trends.
- Establishing and implementing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Maintaining records of reported online safety concerns, including actions.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's online safety procedures.
- Working with the Network Manager to make sure all reasonable precautions are taken to ensure that filtering is age appropriate and set to prevent access to all inappropriate material whilst maintaining all the educational benefits of internet access. *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.*

3.4 The Network Manager

The ICT Network Manager, supported by the DSL, controls internet filtering and monitoring activity and has responsibilities including:

- The day-to-day management and oversight of access and restriction settings that are appropriate for staff and students.
- Maintaining a current record of all staff, students and community users who are granted access to school ICT systems.
- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher and DSL.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Virus protection will be installed and updated regularly.
- Meeting regularly with the DSL to review filtering and monitoring records and implementing any required updates.
- Managing the use of school computer equipment and systems, including internet use, with the network team. Any misuse will be reported by network staff or supervising teachers on ClassCharts and referred to the appropriate Year office for sanctions to be applied.
- Reporting any safeguarding concerns to the DSL/DDSL in line with the school's safeguarding policy.

3.5 Staff

All Springfield staff have the following responsibility:

- Review annually the De Curci Trust 'Acceptable Usage of ICT/Electronic Media policy and re-affirm their commitment to the agreed protocols as well as acceptance of the conditions attached to their personal use of ICT hardware/software.

3.6 Students

Students are responsible for:

- Re-affirming their understanding and acceptance of the 'Student E-Safety Agreement' at the beginning of each academic year.
- Reporting to a member of staff if they receive offensive or worrying e-mails/messages or if they are concerned about something they or a peer have experienced online.
- Taking responsibility for their own safety and the safety of others when working online or on the school network by not revealing personal details or images of themselves or others in electronic communications.

4. Network filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible.

- The school follows the guidance laid out in DfE 'Keeping children safe in education' (September 2024) and DfE 'Filtering and monitoring standards for schools and colleges' (March 2025 update).
- The school takes an active approach to filtering and monitoring all online and network-based activity undertaken by all users
- The school uses appropriate online software to assist with effective filtering and monitoring and the effectiveness of this remains under regular and routine review.
    - All users should be aware that access in school to external personal e-mail accounts may be blocked.
    - The communications of all users using school email addresses and/or other internal messaging services may be monitored.
- In an ever-changing online landscape, the school ensures that filtering and monitoring systems and settings are adjusted as required to ensure the most effective protection for students is maintained. This is regularly reviewed and monitored by the Network Manager and DSL.
- Staff receive regular training and updates by the DSL to ensure they are well informed and well placed to conduct effective monitoring.
- Agreed procedures are in place for the provision of temporary access of "guests" (e.g., trainee teachers and supply teachers) onto school systems. Our procedure for this, which provides temporary access with no email and limited shared area access, unless it's asked for by a member of the senior leadership team in agreement with the network manager.

5. Mobile phones and electronic devices

- Mobile phone use is strictly prohibited during school hours: students are permitted to bring their mobile phone to school but must hand it to their tutor at the start of the school day who will lock it away in a secure cabinet. Students will be able to collect their phones at the end of the school day.
- Any student found to be using a mobile phone/device (or when a mobile phone/device 'sounds' in anyway) will have the phone/device confiscated by the member of staff and the student will be issued with a 60 minute detention.
- Students must never use a phone or device to record (audio or video) another student or member of staff at any time. Failure to comply with this expectation will lead to sanctions up to and including fixed term suspension from school.
- The school does not accept liability for items brought onto the school which become damaged, lost or stolen and would encourage students not to bring expensive items onto the school site.

6. Managing emerging technologies (including generative artificial intelligence)

Emerging technologies will be examined for educational benefit and once approved, a risk assessment will be carried out before use in school is allowed.

6.1 Generative Artificial Intelligence (AI)

There are significant opportunities from advancements in AI. Whilst the technology continues to develop, it is important that the whole school community is aware of the following points:

- AI technology is not a replacement for the subject knowledge or judgement of an expert human.
- There are some benefits such as supporting administration tasks, creating student feedback and the creation of resources. However, staff must be aware of the limitations and risks in using the technology and can only use approved AI software as directed in the emerging AI policy.
- There are safeguarding risks associated with the use of AI technology. AI risks will be taught via the school Personal Development Learning curriculum.
- Teachers should be aware of the guidance published by the Joint Council for Qualifications (JCQ) on the use of AI in assessments. This guidance provides information on how to prevent and identify potential malpractice involving the misuse of AI. The guidance is linked here.

7. Social networking and school published content

7.1 Social networking

- The school will normally block/filter access to social networking and artificial intelligence (AI)/'chatbot' sites unless short-term access is required for a specific educational project.
- Students will be taught the rules and principles for keeping themselves safe online as part of the PDL curriculum.
- Complaints of internet misuse involving cyber-bullying will be dealt with by the Heads of Achievement and recorded in ClassCharts behaviour records.
- All users of social media must be aware of their responsibilities as outlined in the 'Acceptable use' agreements signed on an annual basis.

7.2 School published content

- Contact details and web content are restricted and monitored by a member of SLT.
- Photographs of students involved in school activities or examples of their work may be included on the school's website as stated in the Home-School Agreement and where consent is given.
- If parents/carers wish to withdraw permission then they should put their objections, in writing, to the Headteacher.

8. Equality

The E-Safety policy is intended to enhance values laid out in the Equality Policy by:

- Ensuring that respect for others is considered in all electronic communication and publications.
- Providing a safe learning environment whilst allowing access to as full a range of technologies and social developments as possible.
- Protecting members of the school from any kind of harassment or discrimination using new technologies.
- Ensuring, through policy and practice, that the school has systems in place to effectively challenge, combat and repair discriminatory behaviour towards members of the school community caused by any infringement of this policy or the ICT acceptable usage policies.

9. Linked policies and guidance

This policy must be read in in conjunction with the following key policies and guidance documents:

Teaching Online Safety in Schools' (Updated June 2023)
Keeping Children Safe in Education (September 2024)
Filtering and monitoring standards for schools and colleges (Updated March 2025)
Teachers' Standards (Updated July 2021)
UK Data Protection
Providing remote education: guidance for schools (Updated August 2024)

DCT Acceptable usage of ICT/Electronic Media Policy
DCT Code of Conduct (Staff)
AI Policy (when approved)
Mobile Phone Policy
Safeguarding Policy
School Behaviour Policy
Disciplinary Policy