Online Safety Policy

Derby Grammar School

September 2025

Contents

1 Regulatory framework

1.1 This policy has regard to the following guidance and advice

1.1.1 Keeping children safe in education (DfE, September 2025) (KCSIE)

1.1.2 Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety (UKCCIS), August 2016)

1.1.3 The use of social media for online radicalisation, July 2015

1.1.4 Prevent duty guidance for England and Wales (HM Government, December 2023)

1.1.5 Teaching Online Safety in Schools, (DfE June 2019. Last update January 2023)

1.1.6 UK Council for Internet Safety guidance (various)

1.1.7 Meeting digital and technology standards in schools and colleges (DfE, March 2023)

2 Online Safety

2.1 This Online Safety Policy outlines the commitment of Derby Grammar School 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, learners, 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; this includes our EYFS. It also applies to the use of personal digital technology on the school site (where allowed).

2.2 Derby Grammar School 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.

2.3 Derby Grammar School's Online Safety policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding and Child Protection, Anti-bullying, Behaviour Management, Staff and Pupil Acceptable Use policies and agreements, and Social Media policies. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

2.4 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2.5 Online Safety encompasses not only Internet technologies but also electronic communications such as electronic devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

2.6 The Internet is an open communications channel, available to all. Applications such as the Web, email, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. However, it needs to be used safely.

2.7 Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime, radicalisation, terrorism and religious extremism and racism that would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security. The aim of this policy is to ensure appropriate steps are taken to make the virtual world a safe one for all members of the school community.

2.8 The School will ensure that staff have appropriate training regarding online safety as per KCSIE September 2023. The growth of different electronic media in everyday life and an ever-developing variety of devices including PCs, laptops, electronic devices, webcams etc. place an additional risk on our children. All should be aware of the dangers of sexting of putting children in danger. Internet chat rooms, discussion forums or social networks can all be used as a means of contacting children and young people with a view to grooming them for inappropriate or abusive relationships.

2.9 The best protection is to make pupils aware of the dangers through curriculum teaching particularly Computing ,RHE/PSHE and sex education. Protection is Prevention.

2.10 The breath of issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

2.10.1 **Content:** being exposed to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism**.**

2.10.2 **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.

2.10.3 **conduct**: personal online behaviour that increases the likelihood of, or causes harm for example making, sending and receiving explicit images e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

2.10.4 **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If pupils or staff feel at risk, this can be reported to the AntiPhishing Working Group https://apwg.org

2.11 The DSL and leadership team have regard for **Online Safety within KCSIE 2025.**

2.11.1 The School will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision. The school will be careful to ensure that these systems do not place unreasonable restrictions on internet access or limit what children can be taught with regards to online teaching and safeguarding

2.11.2 The School acknowledges that whilst filtering and monitoring is an important part of schools online safety responsibilities, it is only one part of our role. Children and adults may have access to systems external to the school control such as electronic devices and other internet enabled devices and technology.

2.11.3 It is recognised that with the advancement of 5G that material can be accessed by pupils. Whilst some filters provided by the school will minimize the majority of inappropriate content it is recognized that not all can be accounted for. The teaching in lessons of RHE/PSHE and within the Computing curriculum and external bodies will emphasise what is deemed appropriate or not. Close monitoring of use of electronic devices in-particular for younger pupils will be maintained. If it felt that children are in breach, measures will be put in place to ensure inappropriate content will not be downloaded and the school reserves the right of total confiscation. The police will be involved if there is any criminal element to misuse of the internet, phones or any other form of electronic media.

2.11.4 The School will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively and will support parents and the wider school community (including all members of staff) to become aware and alert to the need to keep children safe online.

2.11.5 Pupils will be encouraged to discuss openly their use of technology and anything which makes them feel uncomfortable. (If this results in child protection concerns the schools designated child protection person should be informed immediately)

2.11.6 Pupils should not give out their personal details, phone numbers, schools, home address, computer passwords etc.

2.11.7 Pupils should adhere to the school policy on electronic devices, which states that all items should be handed in morning registration. In the event of late arrivals, pupils should hand their electronic devices into the office.

2.12 Derby Grammar School's approach to Online Safety is **based on**:

2.12.1 Educating young people to be responsible users of ICT

2.12.2 Guided educational use

2.12.3 Regulation and control

2.12.4 Working in partnership with staff and parents

2.12.5 The DFE publication: Teaching online safety in schools (June 2019)

2.12.6 Education for a connected world

2.12.7 Vulnerable Children in a Digital World - Internet Matters

2.13 Scope of the Policy

2.13.1 The Education and Inspections Act 2006 empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other On-Line Safety incidents covered by this policy, which may take place out of school, but is linked to pupil membership of the school.

2.14 Responsibility Statement and Allocation of Tasks

2.14.1 The day-to-day responsibility for online safety will be delegated to **the Online Safety Officer** to include:

(a) a leading role in establishing and reviewing the school Online policies and documents

(b) ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place

(c) providing training and advice for staff and parents/guardians

(d) liaising with school ICT technical staff

(e) receiving reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments

(f) reporting regularly to the Leadership Team

2.14.2 The Head, Designated Safeguarding Lead and Senior Leaders role within Online Safety:

(a) The Head and Senior Leaders are responsible 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 Officer

(b) The Head and Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant

(c) The Head and Senior Leaders should consider carefully the content of safeguarding related lessons or activities (including online) in PSHE/RHE, as they will be best placed to support any pupils who may be especially impacted by a lesson.

(d) The Head and Senior Leaders will receive regular monitoring reports from the Online Safety Officer

(e) In the event of a serious Online Safety allegation the Head, Safeguarding Officer and Senior Leaders will ensure staff adhere to guidance laid out in the Safeguarding Policy

2.14.3 The Nexus representative who works for Derby Grammar School is responsible for ensuring:

(a) that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

(b) that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

(c) that the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

(d) that they keep up to date with On-Line 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 network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Officer for investigation

(e) that monitoring software / systems are implemented and updated as agreed In school policies

(f) that appropriate handover that is given in circumstances of staff change or termination of contract

2.15 Staff and support staff

2.15.1 Staff are responsible for using the school ICT systems in accordance with the Staff Acceptable Use Policy, which they will be expected to sign before being given access to the school systems. All temporary staff will be required to sign an AUP.

2.15.2 It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

(a) A planned programme of Online Safety training will be made available to staff via Educare

(b) All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school On-Line Safety policy and Acceptable Use Policies

(c) The Online Safety officer will provide advice / guidance / training as required to individuals as required

2.16 Pupils

2.16.1 Pupils are responsible for using the school ICT systems in accordance with the Pupils Acceptable Use Policy, which they will be expected to sign before being given access to the school systems.

2.16.2 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 On-Line Safety is therefore an essential part of the school's On-Line Safety provision. Children and young people need the help and support of the school to recognise and avoid On-Line Safety risks and build their resilience. It is important that we communicate with pupils in a safe and beneficial way, so that pupils remain respectfully cautious but not fearful.

2.16.3 On-Line Safety education will be provided in the following ways:

(a) An Online Safety programme will be provided as part of Computing and RHE/PSHE, this will cover both the use of ICT and new technologies in school and outside school
(b) Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
(c) Pupils will be taught how to evaluate what they see online so that and to be critically aware of the materials and content they access on-line and be guided to validate the accuracy and safety of information
(d) Pupils will be taught how to recognise techniques used for persuasion by looking at false and misleading content
(e) Staff and older pupils should act as good role models in their use of ICT, the internet and mobile devices
(f) Pupils will also be taught how and when to seek support

2.17 Parents

2.17.1 Parents play a crucial role in ensuring that their children understand the need to use the internet and other electronic devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less

experienced in the use of ICT than their children. The school will therefore offer the opportunity for Online Safety training each academic year. Regular Online Safety tips are included in the news letters.

2.17.2 Parents and carers will be responsible for:

(a) endorsing (by signature) the Pupil Acceptable Use Policy

(b) reading the Anti-bullying policy (including On-Line Safety) which is published on the school website

(c) attending Online Safety information events organised by the school

2.17.3 In line with any other disciplinary incident parents will be informed of a breach of the school's bullying policy.

2.18 Data Protection

2.18.1 Personal data will be recorded, processed, transferred and made available according to the GDPR May 2018 which states that personal data must be:

(a) Fairly and lawfully processed

(b) Processed for limited purposes

(c) Adequate, relevant and not excessive

(d) Accurate

(e) Kept no longer than is necessary

(f) Processed in accordance with the data subject's rights

(g) Secure

(h) Only transferred to others with adequate protection

2.18.2 Staff must ensure that they:

(a) At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse

(b) Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

3 Version control

Date of adoption of this policy	September 2025

Date of last review of this policy	September 2025
Date for next review of this policy	Autumn 2026
Policy owner (SMT)	Head and Online Safety Lead
Policy owner (Proprietor)	ILG