

Dartford Grammar School for Girls

ONLINE SAFETY (E-SAFETY) POLICY

DATE REVIEWED: September 2026

NEXT REVIEW DUE: September 2027

Philosophy

Online safety includes internet technologies, data and data storage, and electronic communications such as email, mobile phones, smart watches, digital cameras, social media sites and use of Artificial Intelligence (AI). The school Trust Board, students and parents/carers should work together to understand the issues and risks associated with the use of digital technology for children. New technology has become integral to the lives of young people in modern society. Students should have an entitlement to safe internet access at all times.

This online safety policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. It addresses the need to educate staff, students and parents/carers about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's online safety policy will operate in conjunction with other policies including policies focusing on Behaviour, Anti-Bullying, Special Educational Needs and Disability, Data Protection and Safeguarding and Child Protection.

The risks associated with online activity are embedded in **Keeping Children Safe in Education 2026** and take into account new UK laws to be passed in Spring 2027.

Online safety in school

- The Online Safety Co-ordinator will be a Designated Safeguarding Lead (DSL).
- Online safety depends on effective practice at a number of levels
- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of the online safety policy in both the areas of administration and curriculum, including secure school network design and use
- Having robust filtering and monitoring software in school
- Safe and secure broadband including the effective management of a filtering system
- Monitoring user activity on school and college devices.

Online safety

The breadth of issues is considerable and ever evolving. There are four main areas of risk:

content: exposure to harmful online content, both illegal and inappropriate e.g. pornography, fake news, racism, suicide etc.

contact: exposure to harmful online interaction e.g. grooming, exploitation etc.

conduct: exposure to the sending and receiving of explicit images etc.

Dartford Grammar School for Girls

commerce: exposure to online gambling, inappropriate advertising and scams etc.
Taken from **Keeping Children Safe in Education 2026**

Teaching and learning

- The school has a duty to provide students with quality internet access as part of their learning experience. Internet use will be used to enhance learning.
- Internet use is a part of the curriculum and a necessary tool for staff and students
- The school internet access will be designed expressly for student use, to attempt to protect students from accessing inappropriate material. This will include filtering through a third-party provider, Smoothwall, who are compliant with the DfE “Filtering and monitoring standards”
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Students should be made aware of the UKCCIS digital code and how to report online safety concerns both in school and to outside agencies, e.g. CEOP
- Students will be made aware that they are responsible for their internet use and that they must keep their log-in details and passwords secure
- To protect personal data, students and staff should not leave a computer or any other device logged on when they move away from their desk
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Students and staff will be made aware of copyright law in relation to internet derived materials
- Students and parents/carers will be expected to sign the plagiarism awareness document on entry to the school – copy in student planner
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security
- Staff should guide students in online activities that will support the planned learning outcomes
- Staff should ensure students are aware that websites may share personal data about their users
- Staff should ensure students are aware that criminals operate online scams e.g. fake emails or websites to extort money or valuable personal information
- Staff should take every opportunity to educate students about the significant online risk associated with misinformation, disinformation (including fake news), and conspiracy theories.

Using guidance from The Online Safety Act 2023

Keeping Children Safe in Education 2026

Managing internet access

- The school ICT system’s capacity and security will be reviewed regularly.
- The virus protection will be updated regularly
- Access levels will be reviewed to reflect the curriculum requirements and age of students

Dartford Grammar School for Girls

- The DSL will work with the Network Manager to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access
- If staff or students discover an unsuitable site, it must be reported to the Online Safety Coordinator/DSL
- Any requests for a site to be unblocked must be made by a member of staff in writing. These requests are approved by the Lead DSL or Headteacher who will communicate the changes required to the Network Manager
- The school will do everything they reasonably can to limit children's exposure to risks from the school's IT system

Filtering and Monitoring

Governing bodies and proprietors should ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. They should consider the age range of the students and those who are potentially at greater risk of harm and how they access the IT system.

Taken from **Keeping Children Safe in Education 2026 (page 40)**

- The filtering system is outsourced to Smoothwall
- The filtering system's basic site and keyword lists are DFE-compliant and are maintained and updated by Smoothwall
- Smoothwall will also provide real-time digital monitoring that provides a 24/7 human moderated service that alerts designated staff to students becoming vulnerable
- All alerts will be sent to the Lead DSL
- All students who use a device on the school domain including their own devices, will have their internet usage filtered and monitored
- All students who use a school device offsite will have their internet usage filtered and monitored through Smoothwall software
- As well as Smoothwall software, the school will ensure other forms of monitoring are in place, such as:
 - o physically monitoring by staff watching screens of users
 - o live supervision by staff on console using Veyon management software

Email

- Staff and students are expected to write emails in a formal manner. Emails should be proof-read before sending to ensure language and tone are appropriate
- Students and staff should only communicate with each other online using their school email account
- Students may only use approved email accounts on the school system.

Dartford Grammar School for Girls

- If students receive an offensive email they must immediately report it to a member of staff
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Emails sent to an external organisation should be written carefully and authorised where appropriate before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Use of student images.

- Student photographs can only be published with the permission of the parents/carers.

Social networking and personal publishing

- The school will block/filter access to social networking sites
- Students will be advised never to give out personal details which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email address, social network details, full names of friends, specific interests etc
- Students and parents/carers will be advised that the use of social network spaces outside school should be monitored and social networking sites are often used inappropriately
- Students and parents/carers will be advised of the age restrictions applicable to popular social network sites and strongly encouraged to adhere to them
- Students are not allowed to use their mobile phones in school during the school day. (See “Use of Mobile Phones (and other electronic devices)” below)
- If necessary e.g. on a school visit, staff will be issued with a school phone where contact with students is required
- Staff should never use a personal mobile device to take and/or store images of students
- Staff should be aware that their social media friends may also be friends with DGGs students or their family members and without the appropriate privacy settings, they could read your posts
- Staff should be aware that their reputation could be harmed by what others share about you online e.g. inappropriate posts, photographs or videos.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to Data Protection Legislation

Authorising Internet access

- All staff must read and sign the ‘Staff ICT Acceptable Use Agreement’ before using any school ICT
- All students must read and sign the ‘Student ICT Acceptable Use Agreement’ before using any school ICT
- The school will keep and maintain a record of all staff and students who are granted internet access

Handling online-safety complaints

Dartford Grammar School for Girls

- Complaints of internet misuse will be dealt with promptly by an appropriate member of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Concerns of a safeguarding or child protection nature must be referred to the DSL
- Where online safety has been breached and this is linked to bullying behaviour, this will be reported to the pastoral team for further action

Communicating online safety

- Online safety rules will be posted in all ICT rooms and discussed with the students regularly
- Online safety will be explicit in the Computer Science curriculum and integral to topics in PSHE and assemblies
- Students will be informed that network and internet use will be monitored and can be traced back to the individual user
- Staff should be aware that internet traffic can be monitored and traced to the individual user
- Parents/carers will be made aware of online safety strategies in newsletters
- Parents/carers and students will be made aware of age limits for social media sites, risks associated with social media and the internet, and advice on privacy and security settings in newsletters and Working Together Evenings, including new laws put in place to prevent harm (from Spring 2027)
- Staff and parents/carers should recognise that the distinction between the online world and real life is less marked for children than for most adults. Staff and parents/carers should support them in distinguishing the difference between them
- Students will receive education on online safety in assemblies including elements of Keeping Children Safe in Education 2026 and understanding new laws put in place to prevent harm (from Spring 2027)
- Students will receive information and education on online safety in registration activities

Use of Mobile Phones (and other electronic devices)

Mobile phones (and other devices such as headphones / cameras) are not needed in school and must not be seen, heard or used inside the Black Gates, for any reason. We do not recommend AirPods are brought into school as they are expensive and easily lost. Smartwatches must only be used as a timepiece and never to send messages or emails etc.

The school site, inside the Black Gates, is a mobile-free zone at all times for students. This includes during any clubs or activities after school. During trips, the Trip Leader will outline expectations and students must adhere to these. Filming or taking photographs inside the Black Gates is never allowed and there are serious sanctions in place for this; we are very keen to protect everyone's privacy.

Dartford Grammar School for Girls

Where to put it in school	• in the inside zipped pocket of your blazer (not in the outside pocket) • in your locked locker • in the valuables box (PE/Dance)
Where can use it	▪ you may only look at or use your mobile phone outside the Black Gates
Rule:	▪ mobile phones must not be seen, heard or used inside the Black Gates for any reason, at any time
Trips	▪ your Trip Leader will outline the expectations;
Clubs	• mobile phones may only be used outside the Black Gates, including after school hours
First occasion	• phone confiscated and may be picked up by the student's parent/carer from Reception from 3:20pm • Yellow Card (including Sixth Form) • HoY phone home to advise phone has been confiscated and can be picked up, and that phone is to be handed in for 1 week afterward
Second occasion	• phone confiscated • Orange Card Detention (including Sixth Form) • parent/carer to collect phone from Reception and • phone to be handed in for 2 weeks afterwards
Third occasion	• phone confiscated • Orange Card Detention (including Sixth Form) • parent/carer to collect phone from Reception and • phone to be handed in for 3 weeks afterwards
Fourth and future occasions	• phone confiscated • SLT detention (including Sixth Form) • parent/carer to collect phone from Reception and • phone to be handed in for 4 weeks afterwards

Sixth Form students only may use their mobile phones/headphones inside the Sixth Form Centre. All other expectations for Sixth Form students remain as above

Online bullying

Staff and students should:

- never respond or retaliate to cyberbullying incidents
- staff should report incidents promptly to their line manager and the DSL
- students should report incidents promptly to their parents/carers, Head of Year or the DSL
- save evidence of the abuse e.g. screenshots including the date and time
- actions could include in-school meetings with the perpetrator, reporting the incident to the social networking site, reporting to the police, seeking advice from the local authority or legal advisers

Dartford Grammar School for Girls

Infringements and sanctions for students

Examples of infringements:

- Using mobile phones (or other technological devices) in lessons
- Unauthorised use of email or social networking sites in school

Examples of sanctions:

- Confiscation of property
- After school detention
- An internal isolation (depending on the content)

Examples of infringements:

- Repeated or continual use of mobile phones or devices, email or social networking sites despite being warned
- Accidentally accessing offensive material and not informing a member of staff
- Use of technology to harass another student or make inappropriate comments
- Use of social media for bullying

Examples of sanctions:

- Confiscation of property
- Parents contacted
- Referred to Head of Year and Online Safety Co-ordinator
- Internal isolation
- Suspension

Examples of infringements:

- Deliberately destroying someone's data
- Deliberately destroying someone's personal or school equipment
- Deliberately trying to access offensive or pornographic material
- Use of social media for bullying or unpleasant behaviour towards any member of the community
- Continuing to send emails or messages regarded as harassment or bullying despite being warned
- Use of social media to make comments about other members of the school community, including staff
- Receipt, transmission or use of material that infringes the Data Protection Act or copyright
- Bringing the school into disrepute

Examples of sanctions:

- Confiscation of property
- Referred to Head of Year and Online Safety Co-ordinator
- Parents/carers contacted
- Outside agencies informed, including the police
- Suspension
- Permanent Exclusion

Infringements and sanctions for staff

Examples of infringements:

- Excessive use of internet for personal activities

Dartford Grammar School for Girls

- Breaching copyright
- Serious misuse or damage to any school hardware or software
- Deliberately accessing any material deemed to be offensive, obscene, racist, homophobic etc.
- Bringing the school into disrepute

Examples of sanctions:

- Referral to line manager or Headteacher
- Warning given
- Outside agencies informed including the police
- School disciplinary procedures

If a member of staff is found to have accessed child pornography – the police will be contacted.

Responsibilities for online safety.

All members of the school community are responsible for online safety.

Students should:

- Be aware of the correct research procedures and the need to avoid plagiarism
- Recognise the need to report abuse, misuse of facilities or access to inappropriate materials and how to do so
- Be aware of the school policy on the use of mobile phones and digital cameras, including the policy on the taking of images and cyber-bullying
- Understand that the school policy on online safety covers their actions outside of school where that affects the school community
- Be aware that the school will inform parents/carers of incidents of inappropriate online safety behaviour from both inside and outside the school

Staff should:

- Follow the guidance set out in the Staff Acceptable ICT Use Agreement
- Report any online safety issues to the Online Safety Coordinator
- Ensure that online safety is embedded in their lessons
- Follow the guidance in this document in the Teaching and Learning section on page 2

Parents/carers should:

- Be aware of online safety advice
- Be aware of and involved in their daughter's/son's use of technology outside of school
- Monitor and support their daughter/son in the safe and appropriate use of technology.

The Network Manager should:

- Assist in the resolution of any online safety issues
- Ensure a suitable third-party provider is in place that offers DfE compliant filtering and monitoring

Online Safety Co-ordinator should:

- Monitor the use of school equipment and the tracking of activity on the internet by the school community
- Ensure breaches of online-safety are dealt with promptly and effectively in line with school policies
- Work with outside agencies including the police where appropriate
- Ensure online-safety is embedded in the Computer Science and PSHE curriculum

Dartford Grammar School for Girls

- Arrange online-safety training for staff and students at least every year
- Communicate information to parents/carers every year.