DULWICH COLLEGE
FOUNDED 1619

**ONLINE SAFETY POLICY**

**Introduction**

1.1 New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. IT and online communications can greatly enhance learning but also pose risk.

1.2 Current and emerging technologies used in and outside of College include: websites, email and instant messaging, generative artificial intelligence (AI), blogs, social networking sites, chat rooms, music / video downloads, live streaming, video sharing, gaming sites, virtual reality and augmented reality devices and games, text messaging and picture messaging, video calls, podcasting, online communities via games consoles and mobile internet devices such as smart phones and tablets.

1.3 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

1.4 The College understands the responsibility to educate pupils on online safety issues, to teach them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom where the pupils will likely have unrestricted access to the internet outside College and via mobile networks e.g. 3G/4G/5G etc. It also understands the importance of involving pupils in discussions about online safety.

1.5 We acknowledge that the issues classified within online safety can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content; for example, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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, including those generated using AI and online bullying.

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.6 The College:

- regularly reviews the methods used to identify, assess and minimise online risk;
- examines emerging technologies for educational benefit and undertake appropriate risk assessments before use in College is permitted;
- ensures that appropriate filtering and monitoring is in place and take all reasonable precautions; and
- puts measures in place to ensure that users can only access appropriate material.

1.7 This policy, supported by the ICT Acceptable Use Policies (for staff and pupils), is implemented to protect the interests and safety of the whole College community, including boarders. It aims to provide clear guidance on how to minimise risks. It is linked to the following College policies:

- Safeguarding (Child Protection) Policy;
- Staff Code of Conduct;
- Health and Safety Policy;
- Behaviour policies;
- Anti-bullying policies;
- ICT Acceptable Use Policies (Staff)
- ICT Acceptable Use Policy (Pupils);
- Social Media Policy;
- Use of Generative Artificial Intelligence Policy;
- Mobile Phone and Wearable Device Policy; and
- Data Protection Policy.

**Scope of this Policy**

2.1 This policy applies to all members of the College community who have access to and are users of the College IT systems (including staff and pupils). In this policy 'staff' includes teaching and operational staff, governors, and volunteers.

2.2 This policy covers both fixed and mobile internet devices provided by the College (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) as well as all devices owned by pupils or staff and brought onto College premises (personal laptops, tablets, smart phones and watches, etc).

**Roles & Responsibilities**

3.1 The **Governors** of the College are responsible for periodically reviewing its effectiveness.

3.2 The **Deputy Master Pupils & Safeguarding** is the **Online Safety Officer** and member of staff with overall responsibility for online safety, including to ensure that:

- staff are adequately trained about online safety (which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring);
- staff are aware of the College procedures that should be followed in the event of breach or suspected breaches of online safety; and
- this policy is understood and upheld by all members of the College community and to help the College keep up-to-date with current online safety issues and guidance issued by relevant organisations, including the Independent Schools Inspectorate, the UK Council for Internet Safety, CEOP (Child Exploitation and Online Protection) and children's services.

3.3 The **Computer Services Department** has a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with technical developments. They are responsible for the security of the College's hardware system, its data and for training the College's teaching and administrative staff in the use of IT. They will monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the **Online Safety Officer**.

3.4 All **staff** working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the College's online safety procedures.

3.5 If the College believes that a child or young person is at risk as a consequence of online activity, it may seek assistance from **CEOP (Child Exploitation and Online Protection)**.

3.6 **Pupils** are responsible for using the College's IT systems in accordance with the ICT Acceptable Use Policy (Pupils) applicable to their Year Group, and for letting staff know if they see those systems being misused.

3.7 It is essential for **parents** to be fully involved in the promotion of online safety, both in and outside of College. The College regularly consults and discuss online safety with parents.

**Staff**

4.1 All staff are required to have read and accepted the ICT Acceptable Use Policy (Staff) before accessing the College's systems (usually via the induction process). New staff receive information on Dulwich College's Online Safety, ICT Acceptable Use Policy (Staff) and Social Media policies as part of their induction.

4.2 All staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

4.3 Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

**Duty to report online safety breaches and safeguarding concerns**

5.1 Staff should promptly inform the Online Safety Officer or the Director of IT Services if they suspect or become aware of an online safety breach, except where the case involves safeguarding concerns, in which case the matter should be reported as set out in paragraph 5.2 below.

5.2 Staff must promptly inform the Designated Safeguarding Lead or one of the Deputy Designated Safeguarding Leads if they have any safeguarding concerns about a pupil related to online activity (including sexting, cyberbullying and inappropriate or illegal content). Where appropriate, safeguarding concerns will be reported to relevant agencies (which may include social services, the police and CEOP).

**Online safety in the curriculum**

6.1 IT and online resources are used increasingly across the curriculum. The College believes it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess pupils' understanding of it in all parts of the College.

6.2 The College provides opportunities to teach about online safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside College will also be carried out via Wellbeing, by presentations in assemblies, as well as informally when opportunities arise.

6.3 At age-appropriate levels, and usually via Wellbeing, pupils are taught about how to look after their own online safety, about recognising online sexual exploitation, stalking and grooming, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at the College in accordance with the Safeguarding (Child Protection) Policy. Pupils

can also contact Childline, the Children's Commissioner or the College's Independent Listener. Contact numbers for these are displayed prominently throughout the College.

6.4 At age-appropriate levels, pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. All pupils are taught about respecting other people's information and images.

6.5 Pupils are taught about the impact of cyber-bullying and how to seek help if they are affected by it. Pupils should approach any member of staff for advice or help if they experience problems.

6.6 Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images (including nudes and semi-nudes). In particular, pupils need to recognise the risks attached to publishing their own images and images of others without consent (including those obtained by means of 'upskirting', which is now a criminal offence) on the internet (e.g. on social networking sites).

**Guidance for parents**

7.1 The College seeks to work closely with parents in promoting a culture of online safety. The College will always contact parents if it has any concerns about pupils' behaviour in this area and encourages parents to share any concerns with the College.

7.2 The College will provide information and guidance on online safety by a variety of means (including offering specific online safety guidance at parent forums and other events).

**College email accounts**

8.1 Staff and pupils should immediately report to the Online Safety Officer (or in the case of pupils, their Form Tutor) the receipt of any communication that makes them feel uncomfortable or which is offensive, discriminatory, threatening or bullying in nature. They should not respond to any such communication.

8.2 Email communications through the College network, WiFi and staff email accounts are monitored.

**Use of the internet and social media**

9.1 The College expects pupils and staff to think carefully before they post any information online or repost or endorse content created by other people.

9.2 The College recognises the increasing presence of generative artificial intelligence (AI) technology. Although generative AI is not new, recent advances mean this technology is easily available to pupils to produce AI-generated content such as test, audio, code, images and video simulations. Pupils must only us AI tools in line with the College's Use of Generative Artificial Intelligence Policy.

9.2 Staff and pupils should ensure their online communications do not: (a) place a child or young person at risk of or cause harm; (b) breach confidentiality; (c) breach copyright or data protection legislation; or (d) discriminate against, threaten, bully or harass any individual.

9.3 All internet usage via the College's systems and its WiFi network is monitored. Deliberate access to inappropriate material may lead to disciplinary action.

9.4 Staff should also refer to the Staff Code of Conduct and the Social Media Policy.

**Filtering and monitoring**

10.1 In having due regard for its responsibility to safeguard and promote the welfare of pupils, and to provide a safe environment in which to learn, the College seeks to limit pupils' exposure to online risks through filtering and monitoring systems whose effectiveness is reviewed regularly. The number and age range of the pupils, those who are potentially at greater risk of harm, and the frequency with which pupils access the IT system, along with the proportionality of costs versus safeguarding risks, are taken into consideration.

10.2 The appropriateness of the College's filtering and mentoring systems are informed in part by the College's risk assessment as required by the Prevent Duty.

10.3 In accordance with the Department for Education's filtering and monitoring standards, and in order to fulfil its duty in ensuring the appropriateness of its filtering and monitoring systems (on College devices and College networks), the College:

- has identified and assigned roles and responsibilities to manage filtering and monitoring systems;
- reviews its filtering and monitoring provision at least annually (drawing on guidance including the Department for Education's *Generative AI: product safety expectations*);
- blocks harmful and inappropriate content without unreasonably affecting teaching and learning; and
- has effective monitoring strategies in place that meets the College's safeguarding needs.

10.4 In order to monitor online behaviour and track necessary interventions, the Securus team reviews captures and notifies the College by email (and, if urgent) by telephone where there are safeguarding concerns. The Online Safety Officer also reviews the proxy logs and Securus regularly. Relevant Heads of School are notified of cases where an individual has viewed or created inappropriate content or has engaged in inappropriate conduct online. The Online Safety Officer maintains an Online Incidents Log, which details concerning behaviour and the outcome of interventions.

10.5 Certain websites are automatically blocked by the College's filtering system, which is reviewed on a

regular basis by the Online Safety Officer. If a website being blocked causes problems for College work / research purposes, pupils should contact the Online Safety Officer for assistance.

10.6 Pupils should report to their Form Tutor if they accidentally access materials of a violent or sexual nature whilst using College equipment or whilst using the College network.

---

| | |
|---|---|
| **Policy Owner:** | Deputy Master Pupils & Safeguarding |
| **Last Reviewed:** | September 2026 |
| **Date of Next Review:** | Michaelmas Term 2027 |