

AMDG



DONHEAD PREPARATORY SCHOOL

POLICY ON PUPILS' USE OF ICT, MOBILE PHONES AND OTHER ELECTRONIC DEVICES (inc EYFS)

This policy applies to all pupils, including children in the EYFS, and should be read alongside the school's safeguarding and child protection policy, behaviour policy, anti-bullying policy, staff code of conduct, data protection policy and acceptable-use arrangements. It reflects Keeping Children Safe in Education 2026, the statutory guidance on mobile phones in schools, the Early Years Foundation Stage statutory framework and the Department for Education's filtering and monitoring standards.

ICT IN THE CURRICULUM

Technology has transformed the entire process of teaching and learning at Donhead. It is a crucial component of every academic subject and is also taught as a subject in its own right. All of our classrooms are equipped with electronic whiteboards, projectors and computers. We have an ICT suite in the school and a bank of laptops that staff can book.

THE ROLE OF TECHNOLOGY IN OUR PUPILS' LIVES

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Donhead to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

The school's approach to online safety addresses the four broad areas of risk: content, including exposure to illegal, inappropriate or harmful material; contact, including harmful interaction with other users; conduct, including personal online behaviour that may increase the likelihood of harm; and commerce, including online gambling, inappropriate advertising, phishing and financial scams. Teaching and safeguarding responses will be age-appropriate and will take account of emerging risks, including artificial intelligence and new communication technologies.

ROLE OF OUR TECHNICAL STAFF

Technical staff maintain the school's digital infrastructure and implement the filtering, monitoring, cyber-security and data-protection controls approved by school leaders. They work with the Designated Safeguarding Lead and senior leadership team to review risks, test the effectiveness of controls and respond promptly to concerns. Monitoring must be proportionate, lawful and consistent with the school's privacy information and data-protection responsibilities. Technical staff

report safeguarding concerns immediately to the Designated Safeguarding Lead and report technical or security incidents through the school's agreed procedures.

The governing body or proprietor has overall strategic responsibility for ensuring that appropriate filtering and monitoring systems are in place. A member of the senior leadership team and a governor will be assigned responsibility for oversight of these arrangements. Their responsibilities include reviewing the effectiveness of the provision, considering reports and safeguarding concerns, ensuring that decisions about blocked and permitted content are documented, and confirming that staff understand how to identify and report concerns.

ROLE OF OUR DESIGNATED SAFEGUARDING LEADER

We recognise that online safety is a child protection and safeguarding issue. The Designated Safeguarding Lead has lead responsibility for online-safety concerns and works with the Subject Leader for Computing, senior leaders and the school's IT support provider to ensure that concerns are identified, recorded, assessed and acted upon. This includes reviewing filtering and monitoring information, responding to incidents, supporting staff and ensuring that relevant safeguarding risks are reflected in training, curriculum provision and school procedures.

MISUSE: STATEMENT OF POLICY

If the school becomes aware that a pupil may be at risk because of online activity, the concern must be reported immediately to the Designated Safeguarding Lead and managed in accordance with the school's safeguarding and child protection procedures. The DSL will consider whether advice, a referral or immediate assistance is required from children's social care, the police, CEOP or another appropriate agency. Evidence will be preserved where it is safe and appropriate to do so. Any misuse of technology involving bullying, harassment, abuse or another breach of school expectations will also be addressed under the relevant safeguarding, behaviour and anti-bullying procedures.

INVOLVEMENT WITH PARENTS AND GUARDIANS

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact you if we have any worries about your child's behaviour in this area, and we hope that you will feel able to share any worries with us.

SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT DONHEAD

E-safety is a whole school responsibility, and we adopt the following procedure for the safe use of the internet inside the school:

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe outside the school.
- We value all of our pupils equally. It is part of the ethos of Donhead to promote considerate behaviour.

- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.
- Within the EYFS setting, personal mobile phones, cameras and other electronic devices with imaging or sharing capabilities must not be used to photograph, record or share information about children. Such devices must be stored securely in accordance with the school's procedures. Only school-authorised devices may be used for permitted educational or safeguarding purposes, with appropriate parental consent, secure storage and handling of images, and compliance with the school's safeguarding and data-protection procedures. Any concern about inappropriate or intrusive images or device use must be reported immediately to the Designated Safeguarding Lead.
- Pupils must not use mobile phones or other personal smart technology during the school day, including lessons, movement between lessons, breaktimes and lunchtime. Devices brought to school must be handed in, signed in at the school office and stored securely until the end of the day, when they will be signed out. Any exception must be agreed in advance by the school, be based on an individual pupil's needs or circumstances, and include clear arrangements for permitted use and supervision.

Keeping the School Network Safe

- The school uses filtering and monitoring systems that are appropriate to the age and needs of its pupils and that protect users from illegal, inappropriate and potentially harmful online content without unreasonably restricting teaching and learning. Decisions about content that is blocked or permitted are documented. The effectiveness of the systems is reviewed regularly and following any significant safeguarding incident, change in technology or change in the school's risk profile. Reports and alerts are reviewed by appropriately trained staff and safeguarding concerns are referred promptly to the Designated Safeguarding Lead.
- The IT Department monitors email traffic and blocks SPAM and certain attachments.
- We have strong anti-virus protection on our network, which is operated by the IT Department.

Last reviewed: September 2026

Next review due: September 2027

This policy will be reviewed at least annually and sooner following changes to statutory guidance, relevant legislation, technology, safeguarding risks or the school's filtering and monitoring arrangements. The governing body or proprietor will receive appropriate assurance that the policy and its associated procedures are implemented effectively.