



DAUNTSEY'S SCHOOL

ONLINE SAFETY POLICY

1. Introduction and Scope

At Dauntsey's, the welfare of all pupils is our paramount responsibility. Every adult who works at the school is aware that they share in the duty of care to safeguard and promote the welfare of the pupils, including when they are online. All staff have a responsibility for Online Safety and our approach is to protect and educate pupils and staff in their use of technology and have mechanisms to identify, intervene in and escalate any concerns where appropriate.

Digital technology and the internet are great resources which bring exciting new experiences, learning opportunities and methods of communication. Use of online resources should be positive and inspiring.

However, it is also important that children, parents, and professionals alike are all aware of the need to guard against the risks associated with the internet environment and behave responsibly when using online technologies.

This policy applies to all members of the Dauntsey's community (including staff, pupils, parents and visitors) who have access to and are users of school's IT systems, both in and out of the school. This policy covers both fixed and mobile devices provided by the school, as well as devices owned by pupils or staff and brought onto school premises. The policy, supported by the other relevant policies and documentation listed, seeks to protect the safety of pupils and staff.

2. The Four Cs

Online Safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using digital devices (e.g. text messages, gaming devices, email, social media etc).

In practice, staying safe online is as much about behaviour as it is security. It is essential that children are safeguarded from potentially harmful and inappropriate material online,

and the breadth of issues within online safety can be categorised into four main areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, 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, and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Where pupils or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

3. Other Relevant Policies and Supporting Documentation

The Online Safety Policy should be read in conjunction with:

- Acceptable Use Policy for Pupils/Acceptable Use Policy for Staff
- Data Protection Policy
- Anti-Bullying Policy
- Filtering and Monitoring Policy
- Remote Learning Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Rules, Rewards and Sanctions (including use of mobile phones by pupils)
- Use of Devices in the Classroom Policy

These policies can be found in My School Portal:

<https://dauntseys.myschoolportal.co.uk/documents/51>

At Dauntsey's the DSL and Head of IT use the 360 Safe self-review tool for schools to review the school's approach to online safety and to keep up with the changing harms and risks technology presents

Pupils

The school understands the responsibility to educate pupils about online safety issues, to teach them appropriate behaviours when using the internet and related technologies in and beyond the classroom.

All pupils read and understand the Acceptable Use Policy Agreement for Pupils as part of their joining instructions. This is designed to help pupils understand that they must use school IT systems in a responsible way, to minimise the risk to their safety, the safety of other users, or to the safety and security of the IT systems.

Through Complementary Curriculum lessons the following topics are also covered:

1st Form	<ul style="list-style-type: none">• Sharing Information Online• Privacy• Cyberbullying• Passwords• Visiting Speaker: Karl Hopwood E-Safety expert Childnet International
2nd Form	<ul style="list-style-type: none">• Staying Safe online• Gossip - social media• Child-on-Child Abuse -sharing of nudes and semi-nudes• Cyberbullying
3rd Form	<ul style="list-style-type: none">• Body Image - The effect of social media on our confidence and self esteem• Sexting (Child-on-Child Abuse)• Social Media Pros and Cons - Acceptable Use and Healthy vs Unhealthy behaviours• Cyber bullying• Consent - sharing images/videos - Coercive and Controlling behaviours
4th Form	<ul style="list-style-type: none">• Pornography and the effect on relationships• Child-on-Child Abuse -sharing of nudes and semi-nudes
5th Form	<ul style="list-style-type: none">• Use of mobile Apps at Festivals• Online banking• Visiting Speaker: It Happens
L6th Form	<ul style="list-style-type: none">• Relationship education Staying Safe Online• Gambling• Visiting Speaker: It Happens
U6th Form	<ul style="list-style-type: none">• Use of Mobile Apps to track Financial Matters• Spotting scams etc. - being independent beyond school• Online Contracts for Mobile Phones, TV Providers etc. How to spot issues• Personal Safety in new relationships including Online

Pupils can also access help and resources through the Teen Tips Wellbeing Hub.

4. Pupil Behaviour

In general, pupils are expected to demonstrate responsible behaviour and foster positive relationships when online. They are expected to make the most of online resources to promote both their learning and wellbeing. Pupils should do all they can to make the internet a positive experience for themselves and others and speak out against any inappropriate behaviour they encounter.

Appropriate and inappropriate use of technology is set out in the Acceptable Use Policy for Pupils and Rules, Rewards and Sanctions.

Appropriate safeguarding and/or disciplinary procedures are followed in relation to any incident of misuse of IT equipment or websites or of cyber bullying. The school reserves the right to take action, including when an offence is committed outside of the school, if it harms members of our community or brings the school into disrepute.

During an incident, the searching or confiscation of a device will be done in accordance with the school's Searching of the Possessions of a Pupil Policy and/or the Policy and Procedures to Deal with Sharing of Nudes and Semi-Nudes.

Should any pupil make mistakes in their online behaviour, in addition to any necessary safeguarding or disciplinary processes, they will be afforded the opportunity to reflect on their behaviour and consider the positives and risks of being online and social media and online safety issues such as their feed, digital footprint, legalities around topics like sharing nudes and semi-nudes and online reputation. The aim of such sessions is to encourage pupils to engage with their digital well-being and empower them to make positive changes in how they manage their lives online.

Bullying, harassment, victimisation and discrimination will not be tolerated. Cyber bullying may be defined as repeated, intentional, unprovoked, malicious actions or words via digital platforms which cause distress and make others feel unhappy and insecure.

Cyber bullying can take place through text messages, pictures/videos via mobile phones, phone calls, emails, social media; instant messaging services, websites, gaming platforms and with the use of AI technologies.

Cyber bullying by pupils will be treated as seriously as any other type of bullying, and will be managed through the School's Anti-Bullying Policy and other relevant policies.

If any pupil encounters difficulties online, they should act immediately and seek help, aiming to quickly regain control. All the usual channels for pastoral support apply, including Housemasters/Housemistresses, Tutors, Senior Management Team, Designated Safeguarding Lead and Deputies, the Medical Centre, Chaplain, counsellors, Independent Person, parents, friends and External Agencies.

Extra help with Online Safety issues can be found here:

- [Childline](#) - for support 0800 1111
- [UK Safer Internet Centre](#) - to report and remove harmful online content
- [CEOP](#) - for advice on making a report about online abuse
- [Get Safe Online](#) – for advice on how to protect yourself online Childnet- advice on all key topics
- [Internet Matters](#) – information and guidance on safety settings

Pupils should be aware of the rules around the use of mobile phones and other digital devices as set out in the Acceptable Use Policy for Pupils and the Use of Mobile Phones Around School, both of which form part of the Rules, Rewards and Sanctions.

Access to personal mobile devices and laptops for the school day will vary across year groups and be age appropriate.

The school recognises that in some circumstances, teaching and learning can take place in the Remote Learning Environment. Advice issued to pupils in the Remote Learning Policy which can be found in the link included in Section 3 above.

Below is a list of some key ideas for pupils to help keep themselves and others safe online. Pupils should:

- Be kind to others online and help to create a culture of mutual respect and tolerance for other people's views, avoiding and reporting any language of hate and abuse.
- Think carefully before writing or posting online to consider the digital footprint being created and how the content could be used or reproduced.
- Aim to keep information general, avoiding posting personal information and photographs that could put themselves or others in harm's way.
- Change passwords regularly and never share passwords.
- Complete software updates on all devices.
- Know the identity of those they are communicating with online and never meet up with someone they have met online without a responsible adult being present.
- Ensure camera, microphone and smart speaker settings are secure.
- Ensure privacy settings are correctly set on Apps and social media platforms.
- Know how to report harmful content and do so as appropriate.
- Use available tools to manage screen time and digital wellbeing effectively.
- Use the internet, both at home and at school responsibly and know the law and school rules.
- Remember to ask for and give consent when necessary.
- Be prepared to block and unfollow other users online.
- Think before clicking to open unrecognised or suspicious content.

5. Parents

It is recognised that parents also play an essential role in the education of their children and in the monitoring and regulation of their children's online behaviour. There are opportunities for parents to listen to external speakers:

- Karl Hopwood - Internet Safety (Autumn/Spring Term)
- Deana Pucciot - Pornography (Spring Term)
- 'It Happens' – Drugs (Summer Term)

They can access help and resources through the Teen Tips Wellbeing Hub and the organisations listed above. These are regularly shared with parents on the school's weekly bulletin.

6. Staff

All staff should read the Online Safety Policy and the other policies signposted above. All staff share in the responsibility for the security of school systems and the data they use or have access to.

All staff should model good practice when using technology maintain a professional level of conduct in their personal use of technology, both on and off site.

The school will provide the Online Safety Policy to all members of staff as part of induction and provide appropriate online safety training and updates for all staff, covering the potential risks posed to pupils as well as professional practice expectations. All staff should have an awareness of a range of online safety issues and how they may be experienced by the children in their care and complete any required training.

All staff should be aware that school systems are monitored, and activity can be traced to individual users; staff should be reminded to behave professionally and in accordance with school policies when accessing school systems and devices.

All staff should be aware that their online conduct outside school, including personal use of social media, could have an impact on their professional role and reputation within school.

All staff should report online safety incidents or concerns affecting pupils, colleagues or other members of the school community to the Designated Safeguarding Lead or Deputies.

All staff must keep personal/bring your own (BYOD) devices up to date with software updates and patches and have appropriate and up to date anti-virus software installed and

refrain from installing dangerous or unwanted software on personal devices which are used to access information relating to the school.

All staff should exercise caution when opening emails, attachments and suspicious web links and content. They should also make themselves aware of terms and conditions, privacy notices etc. when signing up to personal online services or using internet-connected devices. This is especially relevant for AI based services, voice activated devices or devices and applications that use video cameras.

All staff should change passwords according to the school's expectations, never share passwords and complete updates on devices as required.

All advice given to staff regarding Safeguarding and the Remote Learning Environment will be made available in My School Portal and can be found on the link contained in Section 3 above.

7. Filtering and Monitoring

Please see the Filtering and Monitoring Policy.

Staff and pupils can access IT Support using <https://helpdesk.dauntseys.org> or 01380 814666.

8. Generative AI

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. We recognise that Gen AI can introduce risks and these risks are reduced through our existing safeguarding, data protection and technical security arrangements.

The school supports the appropriate use of AI to enhance teaching and learning for both teachers and pupils, please see the pupil and staff frameworks for AI use, and follows latest Government guidelines on Gen AI use in education.

Mrs C Jones
Designated Safeguarding Lead (DSL)

Reviewed: September 2026
Next Review: September 2027