DAUNTSEY'S SCHOOL
E-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 E-Safety.

Digital technology and the internet are an amazing resource which bring exciting new experiences, learning opportunities and methods of communication. Use of online resources can be and 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 ICT 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. Definition of E-Safety

E-Safety, also called 'internet safety', 'online safety' or 'web 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 etc).

In practice, staying safe online is as much about behaviour as it is electronic security. When considering the possible ways in which young people in our care are at risk, the Four Cs are a good format to help shape our thinking:

- Content: being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commercialism: being affected by advertising and marketing schemes, which can also mean inadvertently spending money online.

It is also important to consider how the 'Fifth C' of Consent is involved with the areas above.

3. Other relevant policies and supporting documentation

The E-Safety Policy should be read in conjunction with:

- ICT Acceptable Use for Pupils Policy / ICT Acceptable Use Policy for Staff

- Data Protection Policy
- Anti-Bullying Policy
- The Use and Abuse of Technology Policy
- Remote Learning Policy
- Safeguarding and Child Protection Policy
- Policy and Procedures on Child-on-Child Abuse
- The Code of Conduct for Teaching and Support Staff
- Rules, Rewards and Sanctions (Use of Mobile Phones Around School)

These policies can be located here: https://dauntseys.fireflycloud.net/policies-home-page/school-policies

4. 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 are asked to read and understand the ICT Acceptable Use Policy Agreement for Pupils as part of their joining instructions. This is designed to help pupils understand that they must use school ICT systems in a responsible way, to ensure that there is no risk to their safety, the safety of other users, or to the safety and security of the ICT systems.

Through Complementary Curriculum lessons the following topics are also covered:

1st Form	• Sharing Information Online • Privacy • Cyberbullying • Passwords Visiting Speaker: Karl Hopwood E-Safety expert Childnet International
2nd Form	• Staying Safe online • Gossip - social media • Child-on-Child Abuse -sharing of nudes and semi-nudes • Cyberbullying
3rd Form	• 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	• Pornography and the effect on relationships • Child-on-Child Abuse -sharing of nudes and semi-nudes
5th Form	• Use of mobile Apps at Festivals • Online banking Visiting Speaker: It Happens
L6th Form	• Relationship education Staying Safe Online • Gambling Visiting Speaker: It Happens

Pupils can also access help and resources through *Teen Tips*.

5. 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 well-being. 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 ICT Acceptable Use Policy for Pupils.

Appropriate safeguarding and/or disciplinary procedures are followed in relation to any incident of misuse of ICT equipment or websites or of cyber bullying. The school reserves the right to take action, even 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 a Pupil or the Possessions of a Pupil Policy.

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 e-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 phone cameras; phone calls; emails; chat rooms or social networking sites; instant messaging services; bullying via websites; gaming platforms and with the use of deep fake 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, for example the Safeguarding and Child Protection and Child-on-Child Abuse 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 Leads the Medical Centre, Chaplain, Counsellors, Independent Listener, Parents, Friends and External Agencies.

Extra help with E-Safety issues can be found here:

- The website www.thinkuknow.co.uk contains videos, factsheets and other resources
- The following websites offer useful help and advice:
  - 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
  - https://www.getsafeonline.org – for advice on how to protect yourself online
  - https://www.childnet.com/young-people/secondary - advice on all key topics

Pupils should be aware of the rules around the use of mobile phones and other digital devices as set out in the ICT 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, non-exhaustive, 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 well-being 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.

6. 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 Term)
- RAP Project - Pornography (Spring Term)
- 'It Happens' – Pornography and Sharing Images (Summer Term)

They may also access help and resources through Teen Tips 'What Parents Need to Know….', published by National Online Safety. These are regularly shared with parents on the school's weekly bulletin.

7. Staff

All staff should read the E-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 E-Safety Policy to all members of staff as part of induction and provide appropriate E-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 E-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 E-Safety incidents or concerns affecting pupils, colleagues or other members of the school community to the Designated Safeguarding Leads, Second Master or the Bursar.

All staff must keep personal (BYOD) devices up to date with software updates / 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 regularly, 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 on Firefly and can be found on the link contained in Section 3 above.

8. Filtering and Monitoring

The school is primarily a learning environment and as such, balances the rights and freedoms and the accessibility of information for all with robust technical controls for systems and data integrity, safeguarding, anti-radicalisation and data protection.

It is acknowledged that learning by being exposed to an acceptable level of risk is important for all individuals to learn to identify and manage risk for themselves. This is especially important in a school environment.

The school has in place a number of structures to support its commitment to keeping pupils safe online. These include monitoring and controls within the school's networks and access to the internet, restrictions on the use of apps, streaming services and VPNs and robust 'firewalls'.

Reports on internet activity for pupils and staff are generated if needed. Patterns of behaviour and concerns identified by these reports can be escalated and managed through the school's safeguarding or disciplinary procedures. Further education around any issues may also be provided for those pupils involved to help improve their understanding and awareness of E-safety.

Pastoral controls are in place limiting access to some social media, streaming video and gaming content during certain times for pupils.

The key policies and system controls to encourage positive behaviours and limit access to harmful content are as follows:

- Content controls and restrictions on commercial VPNs are in place preventing access to illegal, inappropriate or harmful content and age-inappropriate content, including pornography, self-harm, suicide, misogyny, racism, anti-Semitism, drugs, weapons, radicalisation and extremism.
- Spam filtering, phishing prevention and other technical measures are in place to minimise the exposure of all staff and pupils to inappropriate or risky content on school devices.
- Other technical controls and policies reduce the risk of malware, ransomware, spyware and other unwanted software as far as is practically possible while maintaining rights and freedoms in an education environment.
- Systems to report risky behaviours to the Designated Safeguarding Lead, including age-related risky behaviours in the digital world, are in place.
- Policies on Safeguarding, Bullying and Cyber Bullying, ICT Acceptable Use, Use of Mobile Phones (Rules, Rewards and Sanctions) and Data Protection are all published separately.
- Staff and pupils all have individual credentials and wi-fi keys which they are required to use and not to share.
- Staff have ICT systems training as part of induction or 'on the job' departmental training and relevant staff are required to complete Data Protection training.
- Administration and management staff using specific systems are required to complete cyber-security including phishing training.

- Pupils are exposed to ICT systems and E-Safety material as part of the ICT curriculum.
- Talks and activities are held, with age group targeted content regularly for year groups as part of co-curricular activity.
- Data on pupil internet behaviour and bandwidth usage can be made available in a pastoral care context to enable appropriate discussions to be initiated in the best interests of pupils.

In addition to safeguarding policies and reporting processes and procedures supporting safeguarding, staff and pupils are encouraged to report any E-Safety issues or concerns to ICT support. The School operates a no blame culture in this regard, where issues are resolved, and threats mitigated. We learn from incidents and implement controls and educate to prevent future occurrences or repeat issues.

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

A L Jackson

Deputy Head Pastoral / DSL

Reviewed: September 2022

Next Review: September 2023