DUNRAVEN EDUCATIONAL TRUST

# ONLINE SAFETY AND ACCEPTABLE ICT USE POLICY

---

**What is online safety?**

Online safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically.

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour or exploitation. Many of these risks reflect situations in the non-digital offline world. As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the skills and confidence to face and address these risks.

Safeguarding against these risks is not just an Information and Communication Technology (ICT) responsibility, it is everyone's responsibility, and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

**Policy statement**

The aim of this policy is to ensure staff, students, pupils, Trustees, Governors, volunteers and visitors use the internet and ICT equipment across the Dunraven Educational Trust safely and appropriately. The main areas of risk for our school communities can be summarised as follows:

Content:

- Exposure to illegal, inappropriate or harmful material, including online pornography;
- Ignoring age ratings in games (exposure to violence and inappropriate language);
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- Hate sites; and
- Content validation: how to check authenticity and accuracy of online content.

Contact:

- Being subjected to harmful online interaction with other users;
- Grooming;
- Child sexual exploitation;
- Cyber-bullying in all forms;
- Extremism and radicalisation; and
- Identity theft and sharing passwords.

Conduct:

- Personal online behaviour that increases the likelihood of, or causes, harm;
- Privacy issues, including disclosure of personal information;
- Digital footprint and online reputation;
- Health and wellbeing (amount of time spent online (socialising, watching video or gaming);

- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images); and
- Copyright (no thought or consideration for intellectual property and ownership – such as music and film).

**Scope**

This policy applies to all members of the Dunraven Educational Trust and its schools (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of ICT systems, both onsite and offsite.

The Education and Inspections Act 2006 allows Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy which may take place outside of the school or are linked to the membership of the school or Trust. The Education Act 2011 increased these powers with regard to the searching for and the deletion of data.

The Trust will deal with such incidents within this policy and associated behaviour/anti-bullying policies, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside the schools' premises.

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education September 2018.**

**Communication**

This policy will be communicated to individuals in the following ways:

- It will be posted on the Trust and individual school's websites;
- It will be part of the induction packs for new staff at all schools across the Trust;
- It will be given to pupils at the start of each academic year along with an ICT acceptable use agreements; and
- All pupils and teachers will be required to undertake e-safety training.

**Education and curriculum**

The Trust has a clear, progressive online safety education programme as part of their curriculum, which covers a range of skills and behaviours appropriate to the pupils' age and experience. This includes:

- Developing a range of strategies to evaluate and verify information before accepting its accuracy;
- Raising awareness that the author of a website, blog or post may have a particular bias or purpose, and to develop pupils' skills in recognising this;
- Helping pupils understand how search engines work;

- Demonstrating polite and acceptable behaviour when using software services in an online environment;
- Educating pupils why they must not upload pictures or videos of others without their permission and to know not to download any files – such as video or music files - without permission from the copyright holder;
- Helping pupils develop strategies for dealing with the receipt of inappropriate material;
- Helping pupils to understand why and how some people will 'groom' young people for criminal, anti-social or sexual purposes;
- Educating pupils on the impact of cyberbullying, sexting and trolling, and to educate them on how to seek help if they are affected by any form of online bullying; and
- Educating pupils to report any abuse and how to seek help if they experience problems when using internet-connected technologies.

The Trust will also:

- Plan internet use carefully to ensure that it is age appropriate and it supports the learning objectives for specific curriculum areas:
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons; and
- Ensure that when copying content from the web, staff and pupils understand issues around plagiarism that they must respect and acknowledge copyright and intellectual property rights.

**Staff, Trustee and Governor e-Safety awareness**

The Trust will ensure:

- That staff, trustees and governors know how to send or receive sensitive and personal data, and understand the requirement to encrypt data where the sensitivity of that data requires data protection;
- That regular e-safety training is available to all;
- That as part of the induction process, all new staff, trustees and governors will be provided with information and guidance regarding e-safety and the GDPR.

**Parent e-Safety awareness**

The Trust runs a rolling programme of advice, guidance and training for parents, including:

- An introduction to the Trust's Acceptable Use Policy for new parents;
- Providing information leaflets and updates via school newsletters and the Trust's websites;
- Providing practical presentations/workshops sessions held at schools within the Trust;
- Providing suggestions for safe Internet use including using filtering and parental controls at home; and

- Recommending e-Safety support and information sites to parents.

**Definitions**

**What do we mean by 'online'?**

When we refer to being online we include being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices and games consoles.

**The Trust**

Refers to the Dunraven Educational Trust.

**Parent/carer**

The term parent/carer refers to any individual who has a parental responsibility for a child or has care of a child.

**Use of ICT equipment**

Where pupils are allowed free access to browse the internet, e.g. in break time or after school, staff must be vigilant in monitoring the content of the websites they visit.

Staff, Trustees and Governors who use the Trust's ICT and communications systems:

- Must sign and abide by the Acceptable Use Policy for their respective school
- Must use the systems responsibly and keep them safe;
- Must maintain safe professional boundaries with families. This includes not giving their personal email address to families or pupils or befriending school users on social network and media sites. Staff must also not use their work email for personal use;
- Must keep any passwords provided to allow access to ICT equipment confidential;
- Must ensure the integrity of passwords. Network user account passwords should be strong (with a mixture of letters, numbers and characters) and are to be changed periodically. If a password is compromised, it must be changed as soon as possible;
- Must not install software on the Trust's equipment, including apps, freeware and shareware;
- Must have any use of cloud storage systems (e.g. Dropbox, Google Drive, etc.) approved by the Network Manager;
- Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures; and
- Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on the school's ICT systems;

**Online safety and use of digital devices**

At all times, staff, Trustees, Governors, parents, pupils and volunteers will treat others with respect and will not undertake any actions that may bring the school/academy into disrepute.

Mobile phones, tablets and other digital devices can present a number of problems when not used appropriately, for example:

- Mobile/smartphones, tablets and other personal devices can allow wireless and 3G/4G internet access via alternative ISPs, and thereby bypass the security settings and filtering of schools in the Trust; and
- Mobile/smartphones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture and use or distribution of images of pupils or staff.

**Emails**

Staff should be aware of and follow the separate email policy of their respective school.

**Digital still and video images**

- We gain written parental/carer permission for the use of digital photographs or videos involving their children as part of the agreement form when their child joins a Trust School;
- We do not identify pupils in online photographic materials, or include the full names of pupils in the credits of any published school-produced video materials;
- We encourage a common-sense approach to the use of personal devices. School devices should be used wherever possible for capturing still or video images of pupils. Should personal mobile phones be used, the images must be for school use only and deleted immediately after application. Staff are responsible for checking regularly that this has been done;
- If taking photographs of pupil work for use for classroom materials, similarly the images must be for school use only and deleted immediately after application; and
- Where own devices are used frequently the device should be managed by the member of staff's respective school through tools such as Android Work Mode.

**Data security**

The Trust is responsible for ensuring that all ICT systems are GDPR compliant.

**Mobile phones**

- Staff must take responsibility for their personal mobile phone when they are working with pupils. Use of a screen lock or fingerprint is required for any personal device that has access to the schools email and g-suite. These conditions also apply to volunteers.
- Staff should not use their own personal phones or devices for contacting pupils or their families within or outside of the school in a professional capacity;
- The telephone number of the school should be used by staff in all communication with families, and for emergency contact;
- If staff have no option but to use their personal mobile phone for communication with families, they must prefix the dialled number with 141, in order to hide their phone number;
- Should a situation arise that presents an emergency or safeguarding concern and staff need to use their personal device in order to ensure the wellbeing of a pupil(s) then this will take precedence over general guidance/policies.

**Digital cameras**

- School devices should be used wherever possible to take photos or videos of pupils;
- We gain written parental/carer permission for use of digital photographs or video involving their children as part of the agreement form when their child joins;
- Personal cameras are not allowed in school and should not be used during off-site activities, home visits or outings;
- The use of video equipment can be a legitimate learning/training aid.
- Pupils, volunteers and visitors are not permitted to take photographs or recordings of pupils without permission from the Head of the given school or without prior written consent from the parents/carers;
- No individual is permitted to photograph or record images in the school bathrooms or sports changing areas;
- Photographers will be required to have clear formal identification which must be worn at all times while at the schools; and
- Pupil images will not be used for promotional or press releases unless parents/carers have given prior written consent.

**Internet and social networking sites**

- Internet access across the Trust will always be overseen by a member of staff in each school;
- Pupil access to websites is limited to those agreed by their school only;
- Staff and volunteers will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials on school equipment;
- Staff must not attempt to bypass or evade the school's security systems;
- Staff will report accidental accessing of inappropriate materials in accordance with school procedures;
- The school will never knowingly disclose or publicise personal information relating to pupils on any social media platform without explicit consent. Personal information means data which relate to a living individual who can be identified from that data;
- Staff will be aware that all internet activity, including the use of email, g-suite, records of sites visited (school-related or personal), will be monitored for unusual activity, security and/or network management reasons;
- Staff are instructed not to create or manage social network profiles for pupil use on a personal basis, or to open up their own personal profiles to their pupils or the pupils' families;
- Trust staff will ensure that in private use:
    - No reference is made in social media of pupils, school staff or parents/carers;
    - They do not engage in online discussions on personal matters relating to members of the Trust community or its activities in any negative context, and/or actions that may bring an individual, profession or organisation's reputation into disrepute;
    - Personal opinions should not be attributed to the school or the Trust; and
    - Security settings on staff personal social media profiles are regularly checked to minimise risk lost personal information.

**School websites**

- Pupils' learning and achievements may be published on their school website and Trust social media accounts with agreement from their parents/carers;
- School websites will be edited only by an agreed list of named of staff. All information placed on the websites must adhere to the ethos and values of the respective school and the Trust;
- Personal pupil information, including home address and contact details, will not be uploaded to the school websites;
- The school websites across the Trust will not publish the surnames of pupils;
- Each school will ensure that the image files are appropriately named and do not use pupils' names in any image files if published on the web; and
- Each school will ensure the web hosting company that is used has a published security protocol.

**Online bullying**

Bullying is defined in guidance issued by the Department of Education as: 'behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally.

**What is online bullying?**

Online bullying is the use of technology, for example mobile phone, email, social networking sites, chat rooms, online gaming sites and instant messaging services, to deliberately upset someone else.

Online bullying:

- Can be used to carry out different types of bullying, as an extension of face-to-face bullying;
- Can also go further as it can invade home/personal space and can involve a greater number of people;
- Can be an anonymous method by which bullies can torment their victims at any time of day or night;
- Can draw bystanders into being accessories;
- Includes threats and intimidation; harassment or 'cyber-stalking', vilification/ defamation, exclusion or peer rejection, impersonation, unauthorised publication of private information or images and manipulation;
- Includes sexting and these images can subsequently be widely distributed; and
- Includes trolling which is the practice of posting upsetting, provocative, offensive or off-topic messages within an online community. Trolling comments are posted with the deliberate intent of provoking readers into an emotional response, or disrupting normal on-topic discussion.

**Responding to online bullying**

Most cases of online bullying can be dealt with through anti-bullying policies and procedures. In all cases of online bullying, make sure the evidence of it is preserved. Measures to assist in combating online bullying include:

- The victim changing their mobile phone number;
- The victim reporting the bullying to the site where it was posted;
- Try to get content removed from the given website/platform;
- In some cases, the victim may be able to block the perpetrator from their sites and services;
- Asking the person bullying to remove the offending content and say who they have sent it on to; and
- Contacting the police in cases of actual/suspected illegal content.

**Policy review**

This policy will be reviewed annually or when any significant changes occur regarding the use of technologies within the school.