



E-SAFETY POLICY

Review Date:	Autumn 2020
Reviewed and approved by:	Governing Body
Next review:	Autumn 2021

The Downley School E-Safety Policy

1. Writing and reviewing the e-safety policy

Our e-Safety Policy has been written taking into consideration government guidance and should be read in conjunction with the school's Online Safety Policy and the school's Code of Conduct for Staff.

2. Teaching and learning

Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- An adult will monitor pupils at all times when using the internet.
- Pupils will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be able to gain independent research skills using the internet, which will be overseen by an adult.
- Pupils will be taught how to become good digital citizens

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials and understand what is and is not acceptable.
- Pupils will inform a member of staff immediately if they find material that is inappropriate.
- Any inappropriate material will be shared with the IT co-ordinator for a decision to be made on how to deal with it.

3. Managing Internet Access

Information system security

- The school's IT Co-ordinator, will update virus protection regularly.
- There are a number of wireless points in school.

The Downley School E-Safety Policy

- IT security will be discussed regularly with the school's IT Co-ordinator.

Email

- All staff will have a secure school email account. If pupils are given a secure school email account, they will be taught how to use it in a safe manner as per the AUP.
- When staff cease employment with the school, their accounts will be closed and access to the network will be stopped.
- Pupils must adhere to the AUP and must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site are the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupil's photographs or their work will be carefully selected to ensure that individual pupils are not identified.
- Pupils' full names will not be used anywhere on the Website or the school's Twitter account.
- Photograph permission forms are signed when pupils start school and remain in force for five (5) years from the date it is signed or for as long as the pupil remains at the school. These are held securely at school.

Social networking and personal publishing

- Pupils and parents will be advised to use the internet safely in accordance with the AUP.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported to the IT Co-ordinator immediately.

Managing emerging technologies, mobiles and devices

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The Downley School E-Safety Policy

- Mobile phones will not be used during any formal school time by staff. Mobiles phones should be turned off or put onto silent. Private calls during staff breaks should be made privately and out of earshot of pupils.
- Pupils are not allowed mobile phones in school. If a mobile phone has to be brought to school by a pupil, the class teacher in the classroom will store it. Any mobile phones not handed in will be confiscated and parents will be informed. The sending of abusive or inappropriate text messages is forbidden.
- Photos and recordings can only be transferred to and stored on a school computer before printing.
- In the case of school productions, parents are permitted to take photos of their own child for personal viewing. The school strongly advises against the publication of any such photos on social networking sites.

Protecting personal data

- When leaving a PC unattended all staff and pupils will be asked to lock their workstation until they return.
- Staff are required to keep work laptops and storage devices in a safe place at all times to avoid them being picked up by another party and information viewed or used by others.
- When off the school premises, information viewed on the school network is the staff member's responsibility. Staff are advised to be vigilant with who uses their device and monitor closely what that device is used for.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

Authorising Internet access

- All staff and pupils/parents must sign an 'Acceptable Use Policy' form.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school cannot accept liability for the material accessed, or any consequences of Internet access.

The Downley School E-Safety Policy

- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with schoolchild protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- If staff perform illegal operations using the internet such as viewing pornography the police will be involved.

Community use of the internet

- Parents are able to access the internet using the computers in school (if authorised). Parents will have read and signed the 'Acceptable Use Policy'.
- Parents will be given a password that does not have access to information stored on the network or photographs and digital images of staff and children.

5. Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be discussed with the pupils continually throughout the year.
- E-safety information will be available on display around school.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be asked to read this e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff may only use the internet for personal use outside of directed time.

Enlisting parents' support

- Parents' attention will be drawn to this e-Safety Policy in newsletters and on the school Web site.
- Parents will be offered e-safety advice and information at various times throughout the school year.

Failure to Comply

- Failure to comply with this policy will result in disciplinary action being taken. The Headteacher/Governing Body will investigate all incidents of non-compliance.

The Downley School E-Safety Policy

Please refer to other safeguarding policies, such as the Online Safety Policy for further information

Reviewed Annually by the Governing Body.