



Online Safety Policy

Policy agreed: Autumn 2023
To be reviewed: Autumn 2025

Introduction

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, governors and visitors).

It aims to provide clear guidance on how to minimise risks and how to deal with matters of infringement. It is written to protect all parties.

This e-safety policy is related to other policies including those for bullying, behaviour and child protection. It is the responsibility of the school to ensure that every child in our school is safe. Therefore, we will be as thorough with e-safety as we would be with other aspects of child protection.

Internet use and management

At Dohill Primary School, we recognise that the internet is a vital part of 21st century life for education and needs to be incorporated in all areas of the curriculum. The school has a duty to provide students with the quality internet access as part of their learning. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It is used to raise the standards of education, support professional work of staff and enhance the school's management.

Dohill Primary School uses a 'filtered' Internet Service provided by Telford and Wrekin, which minimises the chances of pupils encountering inappropriate material. We will only allow children to use the Internet when there is a responsible adult present to supervise. We will seek to ensure that internet, mobile phones and other digital technologies are used effectively for their intended educational purpose, within infringing legal requirements or creating unnecessary risk.

E-safety education

Through the teaching and learning of internet safety, we ensure that our children are equipped with the skills and knowledge to overcome and protect themselves from online risks as detailed in the 4Cs.

	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Online Safety will be promoted and developed through key stage assemblies each term, computing lessons, national Internet Safety Days, PSHE and circle times within individual year groups. Consideration and respect will be given to the pupils age, ability and developmental stage. Pupils will be taught Internet use that is acceptable and what is not acceptable and they will be given clear objectives for internet use.

The combination of the site-filtering by Telford and Wrekin, close supervision by teaching staff and the fostering of a responsible attitude in our pupils, in partnership with parents, enables our children to use technology in as safe a way as possible.

Through our NCCE teach computing curriculum scheme, we teach pupils about the vast information resources available on the Internet. Specifically the Digital Literacy element of our curriculum allows pupils to become safe digital users, evaluating websites and recognising the age-appropriateness of software.

Using internet for learning

The internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and as a source of digital learning materials.

Through computing lessons, we teach all of our pupils how to find appropriate information on the internet, and how to ensure, as far as possible, that they understand who has made this information available, and how accurate and truthful it is.

At Dothill Primary, we expect pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school.

- Whether pupils deliberately seek out inappropriate materials or discover it by chance, they will be asked to switch off their computer immediately

and the incident will be reported, so that the Service Provider can block further access to the site.

- Pupils must ask permission before accessing the internet and they should have a clear idea why they are using it.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and research unless permission has been granted otherwise.
- No programmes on disk/CD Rom/USB should be bought in from home for use in school. This is for both legal and security reasons.
- Pupils from all year groups will sign an acceptable user policy agreement.

Managing internet Access

Information system security

- School ICT systems security will be reviewed regularly by the ICT technician from T&W.
- Service Provider (T&W) filters information using Smoothwall (filtering system).
- WiFi access is password protected.
- Staff must use Senso to monitor and control what pupils are typing/accessing during use of computers/laptops to meet safeguarding responsibilities.

Managing filtering

- The school will work in partnership with T&W to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and/or the ICT Technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents on CPOMS will be used to identify patterns and behaviours of the pupils.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to parent email (including Parent Mail texting service) communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as possibly suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and the school web site

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

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will only be published when permission has been granted by the parent/carer of the pupil.
- Pupils' full names will be avoided on the website and social media platforms, particularly in association with photographs.
- Written permission from parents or carers will be obtained as part of the admission process, before photographs of pupils are published on the school website or social media platform.

Social networking and personal publishing on the school learning platform

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised of the age restrictions set for the use of social network spaces outside school.

Managing videoconferencing (if available)

- Videoconferencing will use the Telford and Wrekin network to ensure quality of service and security.
- All videoconferencing will be managed and supervised by the teacher
- Any videoconferencing will be conducted through Microsoft Teams using


staff accounts

Managing emerging technologies

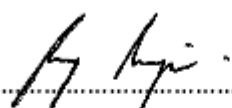
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons and formal school time unless permission has been granted by the Headteacher

Protecting personal data

- Personal data will be processed in accordance with the requirements of GDPR legislation (or equivalent UK legislation).

Signed..........Date 15.11.23

(Head teacher)

Signed..........Date 15.11.23

(Chair of Governors)