Donnington Wood Infant School & Nursery

Online Safety Policy

Date of Policy Creation	**Feb 2018**	**Named Responsibility**	Computing Lead – Mrs C Flint DSL & Headteacher – Mrs C Boddy
Date of review completion	**March 2025**	**Named Responsibility**	Resources Committee
Inception of new Policy	**March 2025**	**Named Responsibility**	Mrs C Flint/Mrs C Boddy
Review date	**March 2027**		
Date of Policy Adoption by Governing Body		March 2025	

All staff will be given a copy of this policy. Copies are available from the office or via the website for parents and members of the wider community.

At Donnington Wood Infant School and Nursery the welfare and well-being of our pupils is paramount. The aim of this policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate use.

This policy must be read in conjunction with –

- Behaviour policy
- Anti-bullying policy
- Child Protection & Safeguarding policy
- Acceptable Use policy
- Mobile Device Policy
- Corporate Information Security Policy

The school's Computing lead, Designated Safeguarding Lead (the head teacher) and Designated Governor for Online Safety will act as the Online Safety team. The school Online Safety team, building on the CEOP and government guidance, has written our e-safety policy. It has been agreed and approved by governors. The Online Safety policy and its implementation will be reviewed every two years.

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 children with quality Internet access as part of their learning experience. Internet use is part of the statutory curriculum and necessary tool for staff and pupils.

Pupils will be taught to use Internet to enhance learning

The school Internet access is designed expressly for pupil use and includes filtering of content. Senso is used to monitor staff and pupil internet usage.

Consideration and respect will be given to the pupils age, ability and developmental stage. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

At Donnington Wood Infant School and Nursery we believe it is vital that children learn, in an age-appropriate way, how to use the internet safely and respectfully. We do this through planned and incidental opportunities. Here are some of the ways we teach and tackle online safety concerns.

- taught curriculum (Computing & PSHE)
- half-termly 'Love of Reading' book about Online Safety (see Appendix 1)
- assemblies
- Staying Safe Superstars
- response to incidents
- response to community concerns

In addition to planned learning within our Computing curriculum, we also use Project Evolve to tailor Online Safety learning for each year group. Project Evolve activities are tailored in response to pupil voice every half term.

We recognise that many children have access at home to internet enabled devices and that partnership with parents is vital. A monthly Online Safety newsletter is sent to all parents to support parental knowledge. Staff are also available to talk to parents about specific issues or concerns.

Managing Internet Access

Information system security

School ICT systems and usage, including security will be monitored and reviewed regularly by the online safety team. Virus protection is updated and monitored regularly by Telford and Wrekin Borough Council. All use of school computer systems is in accordance with the appropriate usage policy and the login/responsible use policy.

For online safety, basic rules of good password hygiene, expert administration and training help to keep staff and pupils safe, and to avoid incidents.

Email

Due to the age of the children in our care, children at Donnington Wood Infant School and Nursery do not have access to their own email addresses. They learn basic skills related to sending emails through Purple Mash 2Email. Here they can learn how to send "emails" using their own personal login and by emailing other children in their class. 2Email on Purple Mash also allows children to do the 2Respond activities, where they email the practice users to complete activities. All emails and 2Respond activities on Purple Mash can be monitored by class teachers. Notifications are sent via the Purple Mash Alerts when children create emails that need approval or when they report an email for being inappropriate.

Staff may only use approved e-mail accounts on the school system. Private emails should not be used on school devices. Emails are fully auditable, trackable and managed by Telford & Wrekin Council on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection. All staff sign to agree to abide by the Acceptable Use Policy.

Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Staff must regularly update their passwords and make sure they follow the Password Policy for creating secure passwords.

School website

The school website is a key public-facing information portal for the school community with a key reputational value. The Head Teacher, Computing Lead, Office Manager and SENDCo will take editorial responsibility and ensure that content is accurate and appropriate. The site is managed internally through TAW and hosted by Umbraco.

The Department for Education has determined information which must be available on a school website. TAW has compiled RAG (red-amber-green) audits to help schools to ensure that are requirements are met. The school website will be audited and checked annually by the computing lead, in accordance with the DfE guidance.

The contact details on the website should be the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published. Photographs that include pupils will be selected carefully and will not include children where parents/guardians have not given permission. Staff are all made aware of those children in their class who do not have photo permission. Pupil's full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or

carers will be obtained for all pupils through the admissions process. This includes permission for the school to take photographs for education purposes and celebration on the school's website. Pupils' work may be published on the Website with the acknowledgement of the pupil.

Cloud based platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning. This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service.

We use the following cloud platforms:

- Microsoft's Office 365
- OneDrive for file storage
- CPOMS
- Scholarpack

The following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud
- The use of any cloud based platform is agreed through our Data Protection Officer to ensure it complies with current GDPR legislation. This must happen before any use of the platform or parental permission is sought.
- Records are kept of all cloud based platforms used and compliance with GDPR legislation.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work

Online activity (including social media)

At Donnington Wood Infant School and Nursery, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

We expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. Guidance is given out to parents and staff to encourage this. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts.

If parents have a concern about the school, we encourage them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 years, but the school sometimes has to deal with issues arising on social media with pupils/students under the age of 13 years. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that, following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise.

Gaming is increasingly popular with young people, resulting in them spending large amounts of their leisure time on games consoles and online gaming platforms, partly because it is immersive and provides freedom that young people might not otherwise feel they have. It also provides social interaction, is creative and it is, of course, fun. Young people can be particularly vulnerable to gaming risks, including spending too much time gaming, missing out on sleep, becoming agitated when not playing, commercial pressures and contact risks with strangers.

Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. Computing lessons and online safety assemblies will address these risks and promote positive behaviours. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking with their children about the apps, sites and games in use and setting limits on with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). Flyers and newsletters are sent home regularly from school to support parents and carers with this.

The school has an official Facebook account. School staff are asked to post regularly to promote events and learning happening in school. We ask parents/carers not to use these channels to communicate about their children. Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils are not allowed to be 'friends' with or make a friend request to any staff, Governors, volunteers and contractors, or otherwise communicate with those in these roles via social media. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the Designated Safeguarding Lead (Headteacher) or to the Chair of Governors if the concern involves the headteacher.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school on social media and be careful that their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute. The serious consequences of inappropriate behaviour on social media are underlined in the Acceptable Use policy. Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). Staff must not follow public accounts of pupils. Exceptions may be made, e.g. for pre-existing family links, but these must be declared to and approved by the Headteacher.

All members of the school community are reminded that, particularly in the context of social media, it is important to comply with the school policy on sharing of photos and videos and permission is sought before uploading photographs, videos or any other information about other people.

Managing filtering

The schools Online Safety team will work with the Local Authority (as ICT services provider) to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Online Safety team who will follow appropriate procedures. The Online Safety team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. A record of these checks will be made.

Managing emerging technologies

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

Staff are expected to abide by the Acceptable Use Policy and Mobile Device Policy. These policies will be updated to reflect emerging technologies.

Protection personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Communication of the policy

Introduction of Online Safety policy to pupils

Online safety rules will be posted on working walls and discussed with the pupils throughout the computing curriculum. Pupils will be informed that network and Internet use can be and will be monitored regularly. The Safety Superstars will meet termly to discuss how best to share important online safety rules with the children. They will feedback this information in the form of posters displayed around school, flyers for parents and discussions with the children during half-termly assemblies.

Staff and the Online Safety policy

All staff will be given access to the Online Safety policy and a digital copy will be available via the school website. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential. All staff will receive a copy of the Corporate Information Security Policy which includes the acceptable use of ICT equipment and systems.

Enlisting parental support

Parent's attention will be drawn to the school online safety guidance in newsletters and the school website. A copy of the schools Online Safety policy will be available on the school website. An opportunity for parents to have a drop in sessions to discuss any online safety concerns will be on going and taken up when necessary. Parents and carers are also sent monthly newsletters with up-to-date computing information and internet safety concerns. Staff will have regular discussions and meetings with parents if/when concerns arise. These discussions will be logged on CPOMS. There is a dedicated logging category on CPOMS for online safety concerns.

Policy decisions

Assessing risks

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

Handling Online Safety complaints

A member of the school's leadership team will deal with complaints of Internet misuse. Any complaints of staff misuse must be reported to the head teacher. Complaints of a child protection nature must be dealt with in accordance with the child protection policy. Pupils and parents will be informed of the complaints procedure. If necessary, discussions will be held with ICT services or Safeguarding Services.

Appendix 1 – 'Love of Reading' books and Computing Curriculum plan for Online Safety

		Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Nursery	love of reading	*Peppa Pig's family computer* ***Using a computer with an adult***	*Webster's bedtime* ***Bedtime routine***	*Screen time is not forever* ***Healthy habits***	*This is how we stay safe* ***Information about online safety***	*Dot* ***Screentime***	*Unplugged* ***Unplugging***
Reception	love of reading	*Winnie & Wilbur and the new computer* ***Using a computer with an adult***	*The screen thief* ***Screentime***	*Websters Manners* ***Being kind online***	*Blackout* ***Unplugging***	*One Upon a time online* ***Various issues***	*Chicken Clicking* ***Trusting information online***
	Computing	Knows that information can be retrieved from computers.		Interacts with age-appropriate computer software	Interacts with age-appropriate computer software	Children recognise that a range of technology is used in places such as homes and schools.	They select and use technology for particular purpose.
Year 1	love of reading	*Hello Hello* ***Screentime***	*When Charlie McButton Lost Power* ***Unplugging***	*'It's a book'* ***Healthy Habits***	*Goodnight Selfie* ***Photographs***	*Penguinpig* ***Trusting information online***	*Troll Stinks* ***Being unkind online***
	Computing	Online safety & computer skills					
Year 2	love of reading	*Old MacDonald had a phone* ***Various issues***	*Webster's friend* ***Trusting information online***	*But it's just a game* ***Video game addiction***	*The day the screens went blank* ***Screentime***	*Monkeycow* ***Password security***	*Goldilocks (A hashtag cautionary tale)* ***Photographs***
	Computing	Online safety and emails		Using the internet			

Appendix 2 - Links to other organisations and resources

CEOP - http://ceop.police.uk/
Childnet – http://www.childnet-int.org/
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
Internet Watch Foundation - https://www.iwf.org.uk/
Kent – Online Safety Resources page
LGfL – Online Safety Resources
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Report Harmful Content - https://reportharmfulcontent.com/
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
ThinkUKnow - https://www.thinkuknow.co.uk/
UK Council for Internet Safety (UKCIS)
UK Safer Internet Centre – https://www.saferinternet.org.uk/

Bullying/Online-bullying/Sexting/Sexual Harassment
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Childnet – Cyberbullying guidance and practical PSHE toolkit
Childnet – Project deSHAME – Online Sexual Harassment
DfE - Cyberbullying guidance
Diana Award – Anti-Bullying Campaign
Ditch the Label – Online Bullying Charity
Enable – European Anti Bullying programme and resources http://enable.eun.org/
Scottish Anti-Bullying Service, Respect me - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour
SELMA – Hacking Hate - https://selma.swgfl.co.uk

Social Networking
Children's Commissioner, TES and Schillings – Young peoples' rights on social media
Digizen – Social Networking
UKSIC - Safety Features on Social Networks

Working with parents and carers
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Internet Matters
SWGfL – Online Safety Guidance for Parents & Carers
Teach Today - resources for parents workshops/education
Vodafone Digital Parents Magazine

Prevent
Childnet – Trust Me
Prevent Duty Guidance
Prevent for schools – teaching resources

Research
Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework