Watling
PRIMARY SCHOOL
A Denbigh Alliance School

Online Safety Policy 2023

At Watling Primary school we aim to:

- have robust processes in place to ensure the online safety of all members of our school community
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our approach to online safety is based on addressing the following 4 key categories of risk:

Content - being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, self-harm, suicide, radicalisation and extremism

Contact - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit others for sexual, criminal, financial or other purposes

Conduct - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

Commerce - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

ROLES AND RESPONSIBILITIES

The Headteacher / Designated Safeguarding Lead and Safeguarding Team

The Safeguarding Team (which includes the Headteacher as the Designated Safeguarding Lead) has responsibility for online safety in school, in particular:

- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- working collaboratively with other members of the school community to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the school child protection policy
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with school policy
- organising staff training on online safety, including regular updates
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the appropriate parties

The Trust Central IT Team

The Trust Central IT team are responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting a full security check and monitoring the school's IT systems on a regular basis
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Staff, Governors and visitors to the school

Staff and Governors and visitors to the school are responsible for:

- maintaining an understanding of this policy
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (Appendix 3) and ensuring that pupils follow the school's terms on acceptable use (Appendices 1 and 2)
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Visitors to the school, including contractors, agency staff, and volunteers who use the school's ICT systems or internet will be made aware of this policy, when relevant.

If appropriate, they will be expected to read and agree to the terms on acceptable use detailed in Appendix 3.

Parents

Parents are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)

The school will raise parents' awareness of internet safety through our normal methods of communication.

This policy will also be made available to parents on our school website.

ONLINE SAFETY IN THE CURRICULUM

All primary schools have a statutory obligation to teach Relationships and Sex Education (RSE) which cover the key building blocks of healthy, respectful relationships, focusing on family and friendships, in all contexts, including online.

Pupils in Key Stage 1 will also be taught to:

- use technology safely and respectfully, keeping personal information private
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will also be taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- how information and data is shared and used online
- that sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

CYBER-BULLYING

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the relevant school policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Please read our Anti-Bullying and Behaviour Policies for further information.

Examining electronic devices

The Headteacher, and any other member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils, and/or
- is identified in the school Behaviour Policy as a banned item for which a search can be carried out, and/or
- is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is and consider the risk to other pupils and staff - if the search is not urgent, they will seek advice from the Headteacher
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- cause harm, and/or
- undermine the safe environment of the school or disrupt teaching, and/or
- commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- they reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- the pupil and/or the parent or carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **NOT** view the image
- confiscate the device and report the incident to the Headteacher or any other member of the Safeguarding Team immediately, who will decide what to do next

STAFF USING WORK DEVICES OUTSIDE OF SCHOOL

Work devices must be used solely for work activities and should not be used in any way which would violate the terms of acceptable use, as set out in Appendix 3.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- making sure the device locks automatically if left inactive for a period of time
- **NOT** sharing the device among family or friends

INCIDENTS OF MISUSE

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the relevant school policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the relevant policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- children can abuse their peers online through:
  - abusive, harassing, and misogynistic messages
  - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - sharing of abusive images and pornography, to those who don't want to receive such content
- physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and other members of the Safeguarding Team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

MONITORING ARRANGEMENTS

The Safeguarding Team maintain records of behaviour and safeguarding issues related to online safety and these are discussed at Trust Safeguarding meetings on a termly basis.

REVIEW OF THIS POLICY

This policy will be reviewed every year by the Headteacher and an annual risk assessment that considers and reflects the risks pupils face online will be carried out.

This will be given high priority because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS & INTERNET AGREEMENT FOR PUPILS AND PARENTS/CARERS

PUPIL NAME:	

When I use the school's IT equipment (like computers or tablets) and the internet, I will:
• ask a teacher or other adult if I can do so before using them
• only use websites that a teacher or other adult has told me or allowed me to use
• tell my teacher or other adult immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• use school computers for school work only
• be kind to others and not upset or be rude to them
• look after the school IT equipment and tell a teacher or other adult straight away if something is broken or not working properly
• only use the username and password I have been given
• try my hardest to remember my username and password
• never share my password with anyone, including my friends
• never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• save my work if I am asked to do so
• check with my teacher or other adult before I print anything
• log off or shut down a computer when I have finished using it
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil)	**Date**
Parent/carer agreement I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date**

Appendix 2: KS2 Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS & INTERNET AGREEMENT FOR PUPILS AND PARENTS/CARERS

PUPIL NAME:	
When I use the school's IT systems (like computers or tablets) and access the internet in school, I will: • always use the school's IT systems and the internet responsibly and for educational purposes only • only use them when a teacher or adult is present, or with their permission • keep my usernames and passwords safe and not share these with others • keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • tell a teacher or other adult immediately if I find any material which might upset, distress or harm me or others • always log off or shut down a computer when I've finished working on it • follow the rules in the school Mobile Phone Statement if I bring a mobile phone to school with me **I will not:** • access any inappropriate websites including social networking sites, chat rooms and gaming sites unless I have been given permission to do so as part of a learning activity • open any attachments in emails, or follow any links in emails, without checking with a teacher or other adult • use any inappropriate language when communicating online, including in emails • create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • log in to the school's network using someone else's details • arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil)	**Date**
Parent/carer agreement I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date**

Appendix 3: Acceptable Use Agreement (staff, Governors and visitors to school)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS & INTERNET AGREEMENT FOR STAFF, GOVERNORS & VOLUNTEERS

NAME:	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • use them in any way which could harm the school's reputation • access social networking sites or chat rooms • use any improper language when communicating online, including in emails or other messaging services • install any unauthorised software, or connect unauthorised hardware or devices to the school's network • share my password with others or log in to the school's network using someone else's details • take photographs of pupils using any personal devices • share confidential information about the school, its pupils or staff, or other members of the community • access, modify or share data I'm not authorised to do so • promote private businesses, unless that business is directly related to the school I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the Designated Safeguarding Lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's IT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed	**Date**