Woodland View Primary School

Online Safety Policy

Status: Voluntary
Date adopted by governing body:
Date for review: Autumn 22

Statement of intent

This policy is intended to ensure pupils at Woodland View Primary School are protected while using digital technologies at the school.

Woodland View Primary School is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by this useful learning tool. Full compliance with this policy will mitigate these risks and help to ensure pupils are safe online.

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety. The DSL attends training regularly to ensure that they understand the unique risks associated with online safety and to ensure that they are confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.

Risks to children

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, 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; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We refer to these four areas of risk when planning our approach to online safety and ensuring that we are safeguarding children against a broad spectrum of potential online harms.

1. Introduction

1.1. While digital technology and the internet provide an exciting opportunity for pupils to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for pupils to engage in unacceptable behaviour, both online and offline.

1.2. In order to keep pupils safe online, and for them to learn how to keep themselves safe online, all pupils and teachers should be aware of relevant skills and strategies needed to ensure digital safety. This ranges from knowing to only use the internet with adult supervision for younger pupils, to strategies for identifying appropriate links for older children.

1.3. Mitigating the risk to pupils created by digital technology and the internet will be ensured through specific safety lessons and will also be embedded within the general curriculum. The digital world is here to stay and it is vital that our pupils are empowered to use it safely and responsibly, developing the skills they need to be responsible users as they move through to adulthood

1.4. Online safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.

1.5. This policy is to work in conjunction with our Safeguarding and Child Protection Policy, Behaviour and Anti-Bullying Policy and Internet and IT Systems Acceptable Use Policy.

2. Definition

2.1. Digital safety encompasses a number of technologies such as computers, tablet computers, collaboration tools, internet technologies and mobile devices.

3. Online safety measures

3.1. Woodland View Primary School internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for primary age children.

3.2. Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

3.3. Lessons using the internet will be carefully planned and the 'access levels' classes and pupils are afforded will be fully considered, taking into account pupil age and curriculum requirements.

3.4. Children using the internet will do so in classrooms (or other appropriate shared areas of the school) during lesson time and with adult supervision. Use of the internet at other times will be the responsibility of the Class teacher to organise and support to ensure this access is safe.

3.5. Key stage 1 pupils are to engage with the internet with teacher/TA observation or direct teacher/TA supervision.

3.6. Pupils will be taught what internet use is acceptable and unacceptable and will be taught how to be positive, safe users of the digital world in a range of different ways. This includes but is not limited to:

- In September, all classes launch their 'safer use' charter that children sign and agree to for safe use of the internet and digital equipment
- Use of the 'SMART' rules and 'CATS'
- An e-safety specific lesson at the beginning of each half term in school
- An assembly once per half term
- Internet safety day
- anti-bullying week focus

3.7. Staff will receive regular online safety awareness information, including but not limited to:

- Staff meeting CPD
- Termly e-safety newsletter with up-dates on latest advice and guidance
- safeguarding training

3.8. Parents will receive regular communications and support to help them make informed decisions about the use of the internet for their child/ren, including but not limited to:

- Annual parental control information booklet
- Monthly online safety newsletter
- Access to a range of supporting information through the school website

3.9. Particular vigilance is necessary if and when pupils are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.

3.10. If the Google images website is used in class, this should be done using the 'safe search' function. Teachers can make judgement calls on whether to allow the use of Google images at all, due to the range of content and possibility for accessing inappropriate material.

3.11. If an online safety incident occurs it will be reported as soon as possible both verbally and by completing an incident form (see appendix) to the DSL and IT Technician. Records will be kept by the DSL. Any incidents will be acted on appropriately and any actions may include:

- Responsive teaching sessions for pupils
- changes to access
- monitoring of filtering systems

4. School Procedures

4.1. Information system security:

- Woodland View Primary School uses a recognised broadband provider with appropriate firewalls and all appropriate filters. (Talk Straight / Netsweeper)
- The security of the information systems and ICT system capacity will be reviewed regularly.
- The virus protection will be regularly updated. There are procedures in place for virus protection to be updated on any laptops used by staff members or students.

4.2. Email and digital communications:

- Only approved school e-mail accounts may be used at school/via the school network. Additionally, pupils must not receive or access personal e-mail accounts.
- Pupils should notify a teacher immediately if they receive an offensive e-mail.
- Pupils should be taught about the dangers involved in e-mail communications. They should be taught:
    - Not to reveal personal details about themselves or others in e-mail or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, instant messenger (IM) address, e-mail address, names of friends, specific interests and clubs etc.
    - Never to arrange to meet someone they have 'met' via e-mail/online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
    - That online communications are 'real' and as such require the same respect for others as face-to-face interactions.

- Parents and pupils alike will both be informed of the risks inherent in using social media.
- Whenever pupils send e-mails to organisations or persons outside of the school, these should be authorised in the same way official school correspondence would be.

4.3. The school website: **www.wvps.northants.sch.uk**

- The Headteacher has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. There are procedures in place for authorising the uploading of any content onto the school's website.
- No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, e-mail and main telephone number should be the only contact information available to website visitors.
- The uploading of any images or photographs of pupils onto the school website requires parental permission, which is included as part of the data collection sheets. Any images should be carefully chosen with safeguarding in mind. Pupil's names will not be used in conjunction with their photograph on the website.

4.4. Managing filtering:

- The ICT Manager will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular checks and ongoing monitoring.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT Manager. There are processes in place to deal with such reports.

4.5. Protecting personal data:

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

4.6. Complaints:

- Complaints regarding pupil misuse of the school's internet/digital devices will be dealt with through the schools behaviour policy.
- Staff misuse of the internet or digital technology should be referred to the Headteacher.
- Any issues or complaints of a child protection nature will be dealt with according to the school's Child Protection and Safeguarding Policy procedure.
- Information on the complaints procedure is published on the school's website and parents are informed of this.

4.7. Digital technology/internet use outside of school:

- Parents will be informed of the inherent risks of internet use.
- The school will be aware of, and responsive to, any issues pupils experience via their use of the internet or digital technology outside of school. The school's Behaviour and Anti Bullying Policy may also be relevant in such instances.

5. Monitoring

5.1. The law related to internet use is changing rapidly and staff and pupils need to be aware of this. Relevant laws include:

- The Computer Misuse Act 1990
- The Public Order Act 1986
- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988
- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997

5.2. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The school business manager and ICT Leaders are responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.

WVPS E-Safety Incident Log Form

Name of person reporting incident:	
Date and time of incident:	
Date incident reported:	
Names of people involved:	
Location and device details:	
Details of incident, including evidence:	
Clarification of the risk or breach e.g. does it relate to safeguarding, bullying, inappropriate content, data protection, copyright, infringement, sexting, etc?	
Initial action taken and current status:	
Resolution of incident:	