Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

Introduction

This policy aims to outline the necessary procedures, behaviours and expectations which will improve the safety of children and staff in relation to the use of computers, mobile devices and any other technology.

We, as a school, recognise the growing concerns which are held by children, parents and educators about the risks and threats posed by technology which is, in many cases, readily available.

At Woodcocks' Well CE (VA) Primary School, we have access to the internet through laptops and iPads. Therefore, this policy aims to ensure that these technologies and devices are used responsibly and safely by both staff and children alike. This policy applies to all children all staff, volunteers, companies, visitors, students, educators and anyone else who may use technology within school.

It is important that children learn how to be safe when they are using new technologies. Whilst blocking and banning is part of our policy, we believe a more sustainable approach is required. We will equip the children with the skills and knowledge they need to use the Internet safely and responsibly, managing the risks wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school, in the home and beyond. The computers are provided and maintained for the benefit of all children, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or around school

Use of digital technologies, devices and the internet within school.

Online Safety is taught through the computing curriculum and lessons dedicated to this are repeated at the beginning of every term.

Online Safety education will also be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities e.g. Safer Internet Day, NSPCC focus days.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Rules for use of ICT systems / Internet will be discuss in all classes.
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

The use of digital technologies, devices and the internet should adhere to the following guidelines. Usage should seek to promote education, learning and engagement and not stray

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

into illegal or harmful usage which causes risk. The school expects all users of the technologies, devices and the internet to understand and follow the policy in order to establish a safe and purposeful basis in which computing and technology can be explored.

Acceptable use

In order to keep children safe online at Woodcocks' Well the following rules apply:

Equipment:

• Do not install, attempt to install or store programs of any type on the computers without permission.

• Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.

• Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.).

• Do not eat or drink near computer equipment.

Security and privacy:

• Do not disclose your password to others, or use passwords intended for the use of others.

• Do not use the computers in a way that harasses, harms, offends or insults others.

• Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.

• Computer storage areas will be treated like school desks. Staff may review files and communications to ensure that users are using the system responsibly.

Internet:

• The Internet should only be used for study or for school authorised/supervised activities.

• Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.

• Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.

• Do not engage in 'chat' activities over the Internet. With the exception of Google Classroom and Class Dojo where children may converse with class teachers about their work.

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

• Never arrange to meet anyone via the Internet. People you contact online are not always who they seem. Electronic communication (Email, text, posts)

• Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.

• Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.

• The sending or receiving of electronic messages containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content.

• Always report such messages to a member of staff.

However, if there are incidents whereby deliberate access to websites, online forums or groups or articles which pertain to any of the following areas has been carried out, then the incident should be reported to the police:

• Images of child abuse

• Adult material which breaches the Obscene Publications Act

• Criminally racist or anti-religious material

• Violence and bomb making

• Illegal taking or promotion of drugs

• Software piracy

• Material related to terrorist activity or propaganda

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

• School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in any relevant Local Authority Online Safety Policy and guidance
• There will be regular reviews and audits of the safety and security of school ICT systems
• Servers, wireless systems and cabling must be securely located and physical access restricted

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

• All users will have clearly defined access rights to school ICT systems
• All staff users will be provided with a username and password

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Data protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	child sexual abuse images
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
	adult material that potentially breaches the Obscene Publications Act in the UK
	criminally racist material in UK
	pornography
	promotion of any kind of discrimination
	promotion of racial or religious hatred
	threatening behaviour, including promotion of physical violence or mental harm
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
	Using school systems to run a private business
	Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
	Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
	Creating or propagating computer viruses or other harmful files
	Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
	On-line gaming (educational)
	On-line gaming (non educational)
	On-line gambling
	On-line shopping / commerce
	File sharing
	Use of social networking sites
	Use of video broadcasting eg Youtube

Cyberbullying

This policy applies to all pupils and should be read in conjunction with Anti-Bullying Policy, The Safeguarding and Child Protection Policy, and the Behaviour Policy.

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or a worrying issue to any member of staff.

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

Cyber bullying can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, to deliberately upset someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target. Cyber Bullying is a form of bullying, although there are some particular features which set it alone from bullying.

The key differences are:-

• Impact – The scale and scope of cyber bullying can be greater than other types of bullying

• Targets and Perpetrators – The people involved may have a different profile to traditional bullies and their targets.

• Location – the 24/7 and anyplace nature of cyber bullying

• Anonymity – The person being bullied will not always know who is attacking them.

• Motivation – Some pupils may not be aware that what they are doing is bullying

• Evidence – unlike other forms of bullying the target of the bullying will have evidence of its occurrence.

Procedures to help prevent cyber bullying

As with all aspects of pastoral care, education lies at the heart of our approach. Issues associated with the appropriate use of ICT are discussed both inside and outside the classroom. All pupils follow a structured programme of ICT where pupils are instructed on the responsible use of technology. Each time a pupil logs on to the school network advice is given with regard to the safe usage of email and the internet. Work in ICT is supplemented by the PSHE program. Where incidents of cyber bullying do occur, they are monitored and recorded in the same way as all other forms of bullying.

Please refer to Anti-Bullying Policy for procedures and sanctions.

Use of mobile phones, cameras and other electronic devices

Pupils at Woodcocks' Well are not allowed to bring mobile phones to school. The only exception is if children, who walk to school need a mobile telephone for personal security. The phone is the pupil's responsibility. The phone must be handed in at the school office on their arrival at school where it will be stored in the office cupboard. It is the pupil's responsibility to retrieve it at the end of the school day. Advice against using mobile devices in an inappropriate way with targeted messages, photographs, social media etc. will be covered in PSHE lessons.

Parents

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

The school has a legal obligation to protect children whilst in the school's care. Parents/visitors are not to use their mobile devices while on school premises in the company of the children. Parents are asked to only take photos of their children at the end of a school performance.

Staff Mobile phones belonging to staff must be stored out of sight of children and kept on silent. Mobile phones are not to be used in the classrooms during lesson times or After-School Care either for receiving or sending personal texts, emails or calls. Mobile phones are not to be used for the taking of photographs. Always use the school iPads.

Staff must not use their personal email to contact parents.

Staff mobile devices kept in school must be locked and password protected.

Staff must lock their computers at all times when not using their computers.

Children are not to use computers that are logged in as staff.

Taking, storing and using images - including Data Protection Laws

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission

Online Safety Policy

- Amendments to policy: January 2024
- Policy effective from: March 2018
- Review date: January 2025
- Full Governing Body

- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

When using communication technologies the school considers the following as good practice:

- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Staff Induction

All new teaching and office staff are given guidance on the School's policy on taking, using and storing images of children. New staff are required to sign that they have read and understood the Online-Safety policy and sign an Acceptable Use Agreement.