

Woodcroft Primary School



Online Safety: Acceptable Use of the Internet and Related Technologies Policy

Date policy last reviewed: September 2024

Signed by:

Craig Tallon

September 2024

Headteacher

Date:

Richard Burrows

September 2024

Chair of governors

Date:

Woodcroft Primary School

Acceptable Use of the Internet and related Technologies Policy

Contents (each element can be read as a separate document)

Policy – online health policy overview

Legal Framework reference

Roles & Responsibilities

Policy – Managing the Internet safely

Policy – Managing email

Policy – Use of digital and video images

Policy – Managing equipment, Personal Devices, Remote Learning & Smart Technologies

Policy – How will Infringements be handled

AUP (Acceptable Use Policy) – Parents

AUP – Pupils

AUP - Staff

Guidance – Safeguarding and protecting children

Guidance – Cyberbullying

Guidance – What do we do if?

Resource - 10 Rules for Responsible IT use

Appendix A: Online harms and risks – curriculum coverage from the DfE's 'Teaching online safety in schools' guidance

WOODCROFT PRIMARY SCHOOL MISSION STATEMENT

'Together Towards Success'

Together we aim for all the pupils, parents/carers and staff, to increase their participation within our school. This is achieved through the development of inclusive cultures, policies and practices. We take account of disability, race and gender to create a secure and accepting community where everyone feels valued.

Towards an outstanding school that provides an enriching and creative learning experience for all pupils. We respond to the diversity of need through our commitment to equality; overcoming potential barriers to learning and setting suitable personalised targets.

Success is expected for every pupil. They should reach their full potential, recognising personal strengths and celebrating the achievements of others; both within the school and its wider community.

Statement of intent

Woodcroft Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Behaviour Policy
- Staff Code of Conduct
- Disciplinary Policy and Procedures
- Virtual School for Online Learning

Roles and responsibilities

The Governing Body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:
 - RSE
 - PSHE
 - Citizenship
 - Computing
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT Co-ordinator to conduct termly light-touch reviews of this policy.
- Working with the DSL and Governing Body to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT Co-ordinator.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Governing Body about online safety.
- Working with the headteacher and ICT Co-ordinator to conduct termly light-touch reviews of this policy.
- Working with the headteacher and Governing Body to update this policy on an annual basis.

Computing Coordinator is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Keeping up-to-date with current research, legislation and online trends.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
-

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum (details of coverage contained in Appendix A: Online harms and risks – curriculum coverage from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about).

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Context:

A definition of online health

"online health is about ensuring children use new technologies in a way which will keep them safe without limiting their opportunities for creation and innovation"

(Source: Yorkshire and Humber Grid for learning)

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use technology in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that technology can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

This document was further updated in line with KCSIE (Keeping Children Safe in Education) 2021. In particular, '**All** staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.' **Keeping Children Safe in Education) 2024 (24)**

Furthermore, Woodcroft Primary School's Acceptable Use of the Internet and Related Technologies document applies the PIES (Policies and Leadership, Infrastructure; Education of Stakeholder Groups and Standards) model¹ for online health.

1

http://www.ictcpd4free.co.uk/pluginfile.php/9691/mod_resource/content/1/360-degree-safe-Structure-Map-%28updated-Sept2013%29.pdf

The technologies (Infrastructure)

IT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- email
- Instant messaging (Facebook Messenger, Whatsapp, Snapchat, etc) often using web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular Facebook, twitter, houseparty, Snapchat, Music.ly, Live.ly, TikTok)
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Gaming Sites (Popular www.games.com, <http://www.pogo.com>, <http://www.bigfishgames.com/> / <http://www.clubpenguin.com>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.spotify.com> YouTube Music/, <http://www.last.fm>)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles with social gaming capabilities) that are 'internet ready'.
- Smart phones with email, web functionality and other mobile applications.
- Smart watches with camera, video email and social networking capabilities.

2. Whole school approach to the safe use of technologies

Creating a safe learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive online health education programme for pupils, staff and parents.

3. Roles and Responsibilities (Policies and Leadership)

Online health is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

Our school Online Health Coordinators are the DSL, the RSE Coordinator & the Computing Managers.

Our online health coordinator ensures they keep up to date with online health issues and guidance through liaison with the Local Authority online health Officer and through

organisations such as Naace and The Child Exploitation and Online Protection (CEOP)². The school's online health coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview of online health issues and strategies at this school. We ensure our governors are aware of our local and national guidance on online health and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online health procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of email;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures (including an awareness of tackling cases of peer-on-peer bullying);
- their role in providing online health education for pupils;

Staff are reminded / updated about online health matters at least once a year.

4. Communications (Education of Stakeholder Groups/Standards)

To Pupils

- An online health training programme is in place to raise the awareness and importance of safe and responsible Internet use, as part of the national online health day (Safer Internet Day).
- Instruction in responsible and safe use should precede Internet access.
- An online health scheme of work will be covered as part of the 2019 Computing Curriculum (developed from the NAACE approved 'Switched On' Computing scheme of work, and using Google's 'Be Internet Legends' scheme), as well as throughout the curriculum whenever digital technologies are utilised.

² <http://www.ceop.gov.uk/>

To Staff

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitoring IT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school online health Policy will be provided as required.

To Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents sign a copy of the Online Safety in the Home Link Book at the beginning of each academic year. They are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Woodcroft Weekly Newsletter
- Online resources

How will complaints regarding online health be handled?

The school will take all reasonable precautions to ensure online health. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by, for example: Teacher/ Learning Mentor / online health Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Our online health Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber-bullying are dealt with in accordance with our Behaviour and Anti-Bullying Policies. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Woodcroft Primary School

Policy: Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. Computing skills and knowledge are vital to access life-long learning and employment; indeed Computing is now seen as a functional, essential life-skill along with English and mathematics, as the subjects inclusion in the National Curriculum indicates. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- secure data exchange between local and government bodies.

In support of this, the government provides a Standards Fund grant to support Local Authorities procure broadband services through local Regional Broadband Consortia (RBC). In London the London Grid for Learning (LGfL) is the RBC. London schools are connected onto this broadband network. The LGfL is part of the National Education Network (NEN). All English maintained schools are expected to be part of the NEN.

The Risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

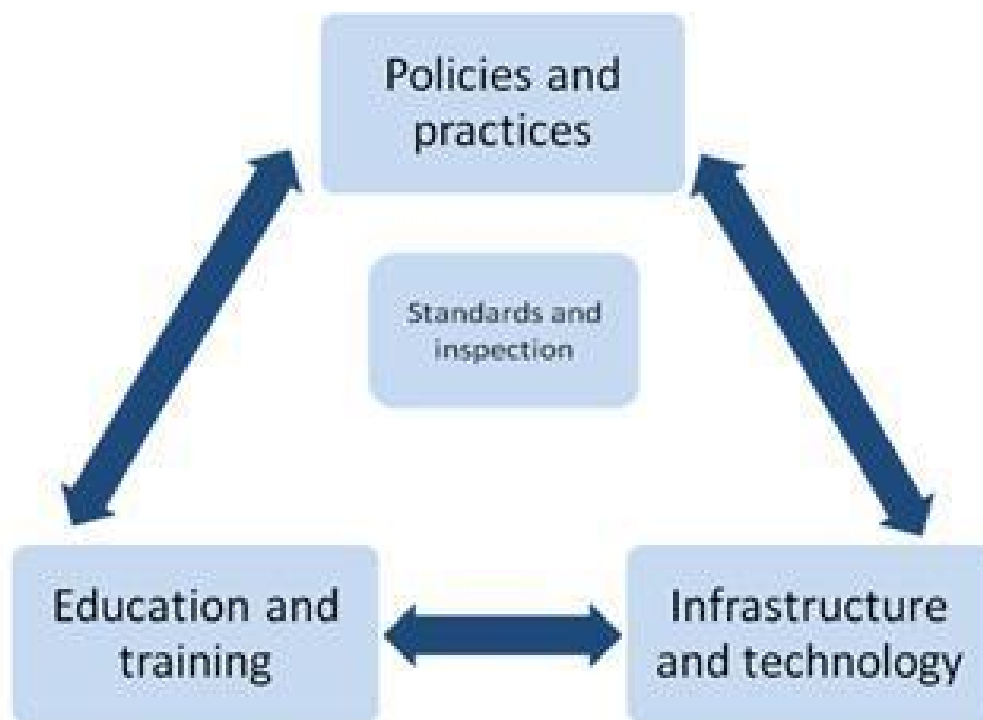
Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse. Risks can be high outside school, so schools should consider extending an education programme to parents and carers.

Schools also need to protect themselves from possible legal challenges. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening emails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Schools help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorized" and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff, (and parents).

There are four core elements for an institution to address when considering the whole school online health NAACE PIES Model. P (Policies and Leadership), I (Infrastructure) and E (Education of Stakeholder Groups) strands, with reference to S (Standards) are detailed below:



Infrastructure:

This school:

- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Has additional user-level filtering in-place using the *Synetrix USO service and G Suite (Google Suite for Education)*.
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot install executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / Network Manager is up-to-date with LGfL/G Suite services and policies;
- Ensures the Systems Administrator / Network Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Uses individual log-ins for pupils from Y3 and all other users;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Restricts pupils to 'safe search' settings;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

Policies and Leadership

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview, where practicable, all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the adult in charge. That adult will then report to the Network Manager. Our systems administrators report to LA / LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;
- Requires pupils (and their parent/carer) from Key Stage 2, to individually sign an online health / acceptable use agreement form which is fully explained and used as part of the teaching programme. Parents of pupils in EYFS & Key Stage 1 sign on their child's behalf;
- Uses closed environments for email with all pupils restricted to email within the woodcroft.barnet.sch.uk domain;
- Requires all staff to sign an online health / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Ensures parents provide consent for pupils to use the Internet, as well as other digital technologies, as part of the online health acceptable use agreement form at time of their daughter's / son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police and the LA.

Education of Stakeholder Groups

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Network Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Teaches an online health programme throughout all Key Stages. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK
 - to discriminate between fact, fiction and opinion;
 - to develop a range of strategies to validate and verify information before accepting its accuracy;
 - to skim and scan information;
 - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - to know some search engines / web sites that are more likely to bring effective results;
 - to know how to narrow down or refine a search;
 - for older pupils, to understand how search engines work;
 - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - for older pupils, to understand why and how some people will 'groom' young people for sexual reasons;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general security issues linked to their role and responsibilities.

Woodcroft Primary School

Policy: Managing email

How will email be managed?

Email is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed email use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects .

However, un-regulated email can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once email is available it is difficult to control its content.

Technology:

Incoming and outgoing email can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. WPS uses the G Suite system which allows key words to be filtered. This list is to be regularly reviewed and updated.

By default any pupil accounts that are created are automatically assigned as 'Woodcroft Domain Only. This means that they can only exchange emails with pupils and teachers from the same school.

Where the school receives nuisance or bullying emails and the email address of the sender is not obvious, it is possible to track the address using 'email' tracking software. Talk to your G Suite Administrator where necessary.

In this school:

- If one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law we contact the police.
- Accounts are managed effectively, with up to date account details of users
- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make email dangerous; G Suite employs world-class filtering systems.

Pupils:

- Pupils can only use school email accounts on the school system.
- Staff can only use school email accounts on the school system.
- Pupils are introduced to, and use email as part of the Computing scheme of work.
- All pupils are introduced to principles of email through closed domain filtering software.
- Pupils are taught about the safety and 'netiquette' of using email i.e.
 - not to give out their email address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
 - that an email is a form of publishing where the message should be clear, short and concise;
 - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
 - they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
 - to 'Stop, Think, Before They Click' and not open attachments unless sure the source is safe;
 - the sending of attachments should be limited;
 - embedding adverts is not allowed;
 - that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
 - not to respond to malicious or threatening messages,
 - not to delete malicious or threatening emails, but to keep them as evidence of bullying;
 - not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
 - that forwarding 'chain' email letters is not permitted;
- Pupils sign the school Agreement Form (via the annual online survey) to say they have read and understood the online health rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use G Suite email systems for professional purposes;
- Access in school to external personal email accounts may be blocked;
- That email sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style';
- Staff sign the appropriate LA / school Agreement Form to say they have read and understood the online health rules, including email and we explain how any inappropriate use will be dealt with.

Woodcroft Primary School

Policy: Use of Digital and Video Images

The School Website.

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to authorised staff;
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual email identities will not be published;
- Photographs published on the web do not have any names attached;
- We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- Digital images/video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials/DVDs without parental permission;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal on the Realsmart VLE in school;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their online health education programme;

Social networking and Personal Publishing

- The schools will block/filter access to social networking sites, except in the case Google+ which is accessible only to staff through G Suite Admin for the purposes of automatic photograph sharing within the schools domain. Staff will be informed of the schools policy of not using Google+ to share images outside the domain, or to use Google+ to connect with outside agencies for anything other than professional purposes.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space, excepting the school's VLE. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs etc. should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be allowed to interact only with others in the school's domain.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Woodcroft Primary School

Policy: Managing Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. In the case of G Suite, the school retains ownership of all content published.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's online health Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with an individual network/G Suite log-in username. From Year 3 they are also expected to use a personal password; prior to Year 3 pupils have password protected access with support of staff or parents.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find; All members of staff have their own unique usernames and are responsible for ensuring they have unique private passwords to access the school's systems.
- Pupils are provided with their own unique username and passwords; class teachers are responsible for ensuring that pupils change their passwords regularly.
- Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.

- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to specific sites. Sites can, however, be unblocked following consultation with Senior Management and the Network Manager.
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted (G Suite) or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school IT systems regularly with regard to security.

Personal devices

Personal devices are used in accordance with the Staff Code of Conduct. Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices capable of capturing images are not permitted to be used in the following locations:

- Toilets
- Changing rooms
- In front of any pupil

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons. If a pupil needs to contact their parents during the school day, they are allowed to use the phone in a public area whilst under the supervision of a minimum of two staff. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated in accordance with the Behaviour Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Remote learning

All remote learning is delivered in line with the school's Virtual School for Online Learning.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Behaviour Policy.

Staff will use all smart technology and personal technology in line with the school's Staff Code of Conduct Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst on school premises.

Where it is deemed necessary, the school will ban pupil's bringing personal technology on school premises.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behavioural Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Woodcroft Primary School

Policy: How will Infringements be handled?

Whenever a student or staff member infringes the online health Policy, the final decision on the level of sanction will be at the discretion of the school management.

Pupils

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

Sanctions: *referral to class teacher, warning given. Woodcroft Primary School Internet Acceptable use Policy for Pupils reiterated.*

Category B infringements

- Continued use of non-educational sites during lessons after being warned.
- Continued unauthorised use of email after being warned.
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups.
- Accidentally corrupting or destroying others' data without notifying a member of staff of it.
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Sanctions: *Referral to Senior Management. Removal of Internet access rights for a period of time. Parents informed. Woodcroft Primary School Internet Acceptable use Policy for Pupils reiterated.*

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or electronic message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Sanctions: Referral to Headteacher. Removal of internet access rights for a period of time. Parents informed. Woodcroft Primary School Internet Acceptable use Policy for Pupils reiterated.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / Synetrix as appropriate

Category D infringements

- Continued sending of emails or electronic messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Deliberate receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Sanctions: Referral to Headteacher in line with the behaviour and Anti-bullying policies. Removal of internet access rights for a period of time. Parents informed. Woodcroft Primary School Internet Acceptable use Policy for Pupils reiterated.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's email service provider

Staff

Category A infringements (Misconduct)

- Excessive use of electronic communication (e.g. Internet, mobile phones etc) for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the internet that compromises the staff members professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful or careless use of passwords. These must be changed from the default and updated (at least termly).
- Breaching copyright or license e.g. installing unlicensed software on network.
- The use of mobile phones in contact time, except in exceptional circumstances authorised by the headteacher.

Sanction - Referral to line manager / Headteacher. Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Deliberate receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute. This includes the use of social media which for non-professional reasons.
- The use of personal mobile phones or other devices capable of storing, distributing and recording images, except in exceptional circumstances authorised by the headteacher.

Sanction – *Referral to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all IT equipment by an outside agency, such as the schools IT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. a technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: <https://www.met.police.uk/ro/report/ocr/af/how-to-report-a-crime/>

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

<http://www.iwf.org.uk>

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's online health / Acceptable Use Policy. All staff will be required to sign the school's Acceptable Use Agreement acceptance form annually;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online health / acceptable use form;
- The school's online health policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on online health issues, (see LGfL safety site).

Woodcroft Primary School
online health agreement form: parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, Google Suite for Education (G Suite) email and other IT facilities at school.

I know that my daughter or son has signed an online health agreement form and that they have a copy of the '10 rules for responsible IT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online health skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online health or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online health.

Parent / guardian signature: _____

Date: ____/____/____

Use of digital images - photography and video: **I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.**

Parent / guardian signature: _____ **Date:** ____/____/____

Woodcroft Primary School

online health agreement form: parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, Google Suite for Education and other IT facilities approved by the school.

I know that my daughter or son has signed an online health agreement form and that they have access to a copy of the 10 'rules for responsible IT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching online health skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online health or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online health.

Parent / guardian signature: _____

Date: ____/____/____

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____ Date: ____/____/____

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we do not use their photograph.

If their photograph is used, we do not name the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.
- Your child's image for presentation purposes around the school;
e.g. in school wall displays and on the school's Virtual Learning Environment (VLE), known as the Treehouse..
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
e.g. on the school's VLE; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Further information for parents on online health can be found at: <http://ceop.police.uk/>

Woodcroft Primary School

Keeping safe: stop, think, before you click!

Pupil name: _____

- ☐ I have read the school 'rules for responsible IT use'. My teacher has explained them to me.
- ☐ I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.
- ☐ This means I will use the computers, Internet, email, online communities, Virtual Learning Environment (VLE), digital cameras, video recorders, and other devices in a safe and responsible way.
- ☐ I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer.

Pupil's signature _____

Date: ____/____/____

Woodcroft Primary School

Digital Technologies Acceptable Use Policy (AUP): Staff

This policy covers the use of digital technologies in school: i.e. email, Internet, intranet and network resources, Virtual Learning Environment (VLE), software, equipment and systems.

I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

I will only use the approved, secure email system(s) for any school business (currently Google Suite for Education (G Suite)).

I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

I will only use the approved, secure cloud-storage system(s) for any school business (currently Google Suite for Education (G Suite)).

I will not browse, download or send material that could be considered offensive to colleagues.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Network Manager or Headteacher.

I will not allow unauthorised individuals to access email / Internet / intranet / network.

I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.

I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended system.

I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.

I will use the school's VLE in accordance with school policy.

I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

I will not engage in any online activity that may compromise my professional responsibilities.

I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.

I will only use LA systems in accordance with any corporate policies.

I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

Digital Technologies Acceptable Use Policy (AUP): Staff

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's IT resources and systems such as Google Suite for Education (G Suite).

Signature Date

Full Name(printed)

Job title

School

Authorised Signature (Head Teacher /Deputy)

I approve this user to be set-up.

Signature Date

Full Name(printed)

Woodcroft Primary School

Guidance: Safeguarding and Protecting Children

What are the online health issues?

Although the use of digital devices and the Internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with.

This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.

An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

The Teachers' Standards 2012 state that teachers (which includes headteachers) should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT Co-ordinators and the headteacher conduct annual light-touch reviews of this policy to evaluate its effectiveness.

The Governing Body, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is Sept 2022.

Any changes made to this policy are communicated to all members of the school community.

Woodcroft Primary School

Guidance: Cyber Bullying

Key national document :
“Cyberbullying – Safe to Learn: Embedding Anti-bullying work in schools”
DCSF-00658-2007

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, emails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (eg: Facebook) or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (such as ‘Happy Slapping’ videos)

It should be noted that the use of digital devices to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997* or the *Telecommunications Act 1984* for example.

What is Bullying?

There are four identifying features of bullying:

- It is deliberate, hurtful behaviour
- It is repeated over a period of time
- It is often difficult for those being bullied to defend themselves
- The bully has and exercises power over the victim.

Bullying can take a number of forms:

- Physical, for example kicking and hitting
- Emotional or verbal, for example name calling, exclusion, threatening or coercion
- Damage to property, for example taking lunches or destroying school books.

All forms of bullying can be damaging to the victim.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

3. *Advise the child not to respond to the message*
4. *Refer to relevant policies including online health/acceptable use, anti-bullying and PHSE and apply appropriate sanctions*
5. *Secure and preserve any evidence* (the school will not copy or transfer evidence, but should secure any devices in question to be passed to relevant authorities).
6. *Inform the sender’s email service provider*
7. *Notify parents of the children involved*
8. *Consider delivering a parent workshop for the school community*

9. *Consider informing the police depending on the severity or repetitious nature of offence*
10. *Inform the LA online health officer*

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. *Inform and request the comments be removed if the site is administered externally*
2. *Secure and preserve any evidence*
3. *Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html*
4. *Endeavour to trace the origin and inform police as appropriate*
5. *Inform LA online health officer*

The school may wish to consider delivering a parent workshop for the school community

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear. “

Woodcroft Primary School

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the Network Manager and ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
 - Remove the PC to a secure place.
 - Instigate an audit of all IT equipment by the schools IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (contact Personnel/Human Resources).
 - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
 - Contact the local police or High Tech Crime Unit and follow their advice.
 - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online health, anti-bullying and PSHE.
3. Secure and preserve any evidence.
4. Inform the sender's email service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA online health officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA online health officer.

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents (using MyConcern).
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.
5. Inform LA online health officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and online health officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the Internet or mobile technology: they must be able to do this without fear.

10 rules for responsible IT use

Keeping safe:

Stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others.

1. I will keep my password secret.
2. I will only use the school's computers to help me learn.
3. The messages I send, or information I upload, will always be polite and sensible.
4. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.
5. I will only email people I know, or my teacher has approved.
6. I will only delete my own files.
7. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
8. I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
9. I will not give my home address, phone number, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.

Think Before You Click

Woodcroft Primary School

S

I will only use the Internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult.

My Name:

My Signature:

Appendix A: Online harms and risks – curriculum coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about.

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong,	This risk or harm is covered in the following curriculum areas:

	misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• Relationships and health education • Computing
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	This risk or harm is covered in the following curriculum areas: • Relationships education

Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • Relationships education
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum areas: • Relationships education
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing

	How to limit the data companies can gather	
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: - That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible - How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: - How to find information about privacy settings on various devices and platforms - That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: - Relationships education - Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: - How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts - How the targeting is done - The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum areas: - Relationships education - Computing

How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm is covered in the following curriculum areas: • Relationships education
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into	This risk or harm is covered in the following curriculum areas:

	offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	• Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing

Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum areas: • Health education • Computing
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour	This risk or harm is covered in the following curriculum areas: • RSE

	That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: - That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with - How to identify indicators of risk and unsafe communications - The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before - What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: - Relationships education - Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: - The issue of using image filters and digital enhancement - The role of social media influencers, including that they are paid to influence the behaviour of their followers - The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: Health education

Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum areas: • Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would	This risk or harm is covered in the following curriculum areas: • Relationships education

	not necessarily be unkind to someone face to face	
--	--	--