METROPOLITAN BOROUGH OF CALDERDALE

Woodhouse Primary School

Daisy Road, Brighouse, West Yorkshire HD6 3SX
Tel : 01484 714750
Email: admin@woodhouse.calderdale.sch.uk

Headteacher: **Mrs Anne Crane**
Deputy Headteacher: **Mrs Smaldon**
Assistant Headteacher: **Mr Freeman**

E - SAFEGUARDING POLICY	
November 2024	

	Date Written/Amended	Next Review Date
Adopted	March 2019	
Reviewed	January 2021	
Reviewed	November 2024	
Next review date	November 2025	

Table of Contents

WOODHOUSE PRIMARY SCHOOL

CURRICULUM AND ASSESSMENT DOCUMENTATION

eSAFEGUARDING POLICY – September 2024

---

1. Introduction

Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their eSafeguarding policies, ensure that they meet their statutory obligations to ensure that children and young people are safe protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors

- Establish clear expectations for the way all members of the school community engage with each other online

- Support the school's policies on data protection, esafety and safeguarding

- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems

- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Code of Conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018

- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Computer Misuse Act 1990

- Human Rights Act 1998

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Education Act 2011

- Freedom of Information Act 2000

- Education and Inspections Act 2006

- Keeping Children Safe in Education 2024

- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre (NCSC): Cyber Security for Schools](#)
- [Education and Training (Welfare of Children) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)

3. Rationale

The use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Long term legacy of digital footprint and online reputation
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying (child on child abuse)
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this eSafeguarding policy is used in conjunction with other school policies (e.g. Behaviour and Discipline, Anti-bullying and Child Protection and Safeguarding procedures, Staff Code of Conduct).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

4. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or other agreed purpose.

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

- **Materials:** files and data created and/or using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology

5. Aims of the Policy

- To set out the key principles expected of all members of the school community at Woodhouse Primary School with respect to the use of technologies

- To safeguard and protect the children and staff of Woodhouse Primary School

- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice

- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use

- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken

- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils

- To develop a partnership approach to Internet learning with parents, including Internet Access Guidelines

- To use ICT to discover, communicate and create

6. Scope of the Policy

This policy applies to the whole school community including the governors, the pupils, volunteers and all staff employed directly or indirectly by the school. This policy also has scope outside of the physical building with regards to online conduct and digital communications.

7. Communication

The Leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.

The eSafeguarding policy will be provided to all members of staff annually. Copies are made available on the school network, and on the school website.

All amendments will be published, and awareness sessions will be held for all members of the school community.

Any amendments to pupils Acceptable Use Policy (AUP) will be discussed with each class to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.

An eSafeguarding module will be included in the RESPECT curriculum and eSafeguarding will be part of the Computing curriculum across the school.

Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.

The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.

The Acceptable Use policy will be discussed with pupils at the start of each school year

8. Roles and Responsibilities

The following section outlines the roles and responsibilities for eSafeguarding of individuals and groups within the school:

8.1 Headteacher and Senior Leaders:

The headteacher is ultimately responsible for eSafeguarding provision for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the IT manager.

The headteacher and senior leadership team are responsible for ensuring that the IT Manager and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.

The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.

The Headteacher will receive reports of eSafeguarding incidents and create a log of incidents to inform future eSafeguarding developments.

The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

8.2 IT Manager:

The IT manager will take day to day responsibility for eSafeguarding issues and has a leading role in establishing and reviewing eSafeguarding policies / documents within the school.

The IT manager will ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident taking place.

The IT manager will ensure, so far as it reasonably practical, that the school's ICT infrastructure is secure and is not open to misuse or malicious attack from both internal and external sources.

Ensures that the school meets the eSafeguarding technical requirements outlined in this policy and Acceptable Usage Policy and any relevant Local Authority Safeguarding Policy and guidance.

Ensures that users may only access the school's networks through a properly enforced password protection policy, with an exception for devices that do not support this such as tablets and mobile phones.

Ensures that the schools internet connection, filtering and firewall is monitored, and the relevant supplier is informed of any issues.

Provides training and advice for staff as and when required.

Liaises regularly with the school's computing lead, Local Authority and other stakeholders as required.

Attends relevant meetings as required.

Reports regularly to Senior Leadership Team.

8.3 Computing Subject leader will:

Have a leading role in establishing and reviewing the school eSafeguarding policies and procedures

Communicate regularly with school technical staff

Communicate when required with the designated Safeguarding Governor

Communicate regularly with the senior leadership team

Ensure that eSafeguarding is promoted to parents and carers

Be responsible for the planning & progression of computing throughout the school

Ensure teaching of eSafety is progressive and pertinent and is visible throughout school.

Monitors ICT activity in lessons, appropriate extracurricular and extended school activities.

Ensure all pupils receive the required eSafety curriculum and that eSafety is embedded in to all computing lessons.

8.5 Teaching and Non-teaching Staff:

Teachers and non-teaching staff are responsible for ensuring that:

They read, understand and help promote the school's eSafeguarding policies and guidance

They read, understand, sign and adhere to the school staff Acceptable Use Policy (Appendix 2)

They report any suspected misuse or problem to the IT Manager

They develop and maintain an awareness of current eSafeguarding issues and guidance

They model safe and responsible behaviours in their own use of technology

They ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones

eSafeguarding messages are embedded in learning activities across all areas of the curriculum.

Pupils are supervised and guided carefully when engaged in learning activities involving technology

Pupils are fully aware of research skills relating to electronic content such as copyright laws

They are aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices

They understand and are aware of incident-reporting mechanisms that exist within the school

They maintain a professional level of conduct in personal use of technology at all times

8.6 Designated person for child protection (DSLs):

The designated person for child protection should be trained in eSafeguarding issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying (child on child abuse)

They shell be familiar with the filtering and monitoring used by the school.

8.7 Responsibilities of Pupils:

To be responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (Appendix 1), which they will be expected to sign before being given access to school systems (KS2 – individually, KS1 on the class document). In YR, Y1 and Y2 pupils sign an A3 class copy which is subsequently displayed in class throughout the year. In KS2 pupils have a copy in their Computing folder which is signed in Y3 and then re-read in Computing lessons every September and throughout the year.

To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

To understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

To understand the importance of adopting good eSafeguarding practice when using digital technologies out of school and realise that the school's eSafeguarding Policy covers their actions out of school, if related to their membership of the school.

To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

8.8 Responsibilities of Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website / Purple Mash and information about national / local eSafeguarding campaigns / literature through appropriate training.

Parents and carers will be responsible for:
- Reading the Parent Acceptable Use Policy (Appendix 3).
- Accessing the school website / Purple Mash and other online systems in accordance with the relevant school Acceptable Use Policy.
- Support the Code of Conduct during periods of remote learning

8.9 Responsibilities of Governors

To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance

To develop an overview of the benefits and risks of the internet and common technologies used by pupils

To develop an overview of how the school ICT infrastructure provides safe access to the internet

To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school

To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities

To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

8.10 Community Users

The school will provide an Acceptable Use Policy for any guest who demonstrates a need to access the school computer system or internet on school grounds.

The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and school ICT equipment.

Internet for guest users will be filtered but not monitored with no SSL filtering due to technical limitations.

9. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Online gambling, inappropriate advertising, phishing and/or financial scams

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful

- Consensual and non-consensual sharing of nude and semi-nude images of and/or videos and/or livestreams

- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Unauthorised sharing of confidential information about the school, its pupils, or other members of the school community

- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data

- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- Causing intentional damage to the school's ICT facilities

- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation

- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

- Using the school's ICT facilities to breach intellectual property rights or copyright

- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):

  - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time.

9.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

- Pupils may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas

- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Exemptions are also in place for authorised personnel carrying out their duties including the sharing of inappropriate content with SLT or investigative bodies.

10. Managing Digital Content

Digital Content includes:

On the school website or blog; in the school prospectus and other printed promotional material, e.g. newspapers; in display material that may be used off site; Recorded or transmitted on a video or via webcam in an educational conference.

We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Pupils and staff will only use school equipment to create digital images, video and sound recordings. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. Images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text if published; such resources will not be published publicly online without the permission of the staff and pupils involved.

Parents may take photographs at school events: however, they agree that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.

When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

11. Guidelines for Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

eSafeguarding education will be provided in the following ways:

Online safety is embedded throughout the curriculum however it is particularly addressed as part of the Computing curriculum and the bespoke RESPECT curriculum.

We promote e-safety through a planned programme of assemblies and whole-school activities, including having a team of digital leaders and promoting Safer Internet Day each year.

We will provide a series of specific online safety lessons in every year group at the start of the year within the context of Computing as a subject. This aims to give pupils the underpinning knowledge of aspects of the online world to help them develop behaviours that can navigate safely and confidently regardless of the device platform or app they're using. It also aims to help pupils develop appropriate scepticism and reasoning when they encounter new online experiences to be able to evaluate the risks or potential pitfalls of these encounters. We further reinforce and expand this teaching through the RESPECT curriculum which also covers aspects of online safety.

The underpinning knowledge and behaviours pupil learn through the curriculum include the following:

- Effective searching and evaluating what they see online.
- Recognising techniques used for persuasion.
- Copyright in relation to online resources.
- Clear understanding of acceptable an unacceptable online behaviour.
- Identifying online risks.
- How to seek support if they experience problems when using the internet and technology.

We supplement this teaching with whole school online safety awareness and through role modelling and discussions in the day-to-day life of the school. We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and which will be displayed across the school.

12. Education & Training – Staff

It is essential that all staff receive eSafeguarding training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

Staff receive regular information and training on eSafeguarding issues in the form of staff meetings and staff training days.

As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.

All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.

The IT Manager will provide advice, guidance and training to individuals as required.

12.1 Training – Governors

Governors should take part in eSafeguarding training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / eSafeguarding / health and safety / child protection.

13. Managing ICT Systems and Access

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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafeguarding responsibilities:

- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware and will be kept active and up to date.
- All users of school systems have internet access by default. The school use a series of rules to determine the level of internet access, these include;
    - o User Type – Pupil, Staff, VPN User, Elevated
    - o The device in use - Server, Admin Device, Tablet, device connected to projector.
    - o The time of day. Slightly stricter controls are in place during the school day compared to before and after school.
    - o There is an option available for 'raw' internet access usually for accessing specific service such as remote support, server management, troubleshooting applications or researching sensitive / security topics and headless devices.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

- At Key Stage 1, pupils will access the internet using a shared class username and password, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

- At Key Stage 2, pupils will have an individual username, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session. Pupils in Years 5 and 6 will be responsible for their own passwords which they are expected to know and keep secure in keeping with the principles of eSafeguarding.

- Members of staff will access computers, and thereby the internet, using an individual username and password, which they will keep secure. They will ensure that they log out after each session or lock their PC and not allow pupils to access the PC through their username and password unless to use the IWB as part of a supervised classroom activity. They will follow the school AUP.

- The school has a number of devices without user accounts, iPads being the most common. These do not allow for users to login and therefore we cannot link internet usage to an individual. They are specifically assigned as either for staff or pupils. The sites visited and search terms used are still recorded and can still be linked to a device.

14. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls

- Security features

- User authentication and multi-factor authentication

- Anti-malware software

14.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for saving accounts and files they create and manage in the right location and ensuring they are maintained and updated.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All access to school information assets will be controlled via username and password where ever practical.

Information systems require end users to change their password at first log on, where practical.

All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords,

Access to personal data is controlled in line with the school's personal data policy.

The school maintains a log of user activity on key systems.

Users should create different passwords for different accounts / applications.

Complex password are easy to generate but difficult for user to remember and type correctly. A new approach is to use three well-chosen random words that can be quite memorable but not easy to guess. It provides a good compromise between protection and usability. The 3 word combined must be at least 12 characters. They could be separated by special characters.

Computer passwords never expire but users can to change them when they wish and must if they suspect their password has been compromised.

Security is enhanced with through the use of Multi-Factor Authentication (MFA) where users outside of school are required to approve a login attempt via an app or entering a code from an app.

Where the level of access if privileged, a MFA challenge will take place regardless of location.

The school use Azure AD with Active Directory Sync which enable simplified sign on to some services. This links Domain (in school) and email passwords so users have one less to remember. They sign in with Microsoft option is then offered on a number of other platforms reducing the number of passwords required and protecting those account with already established MFA.

Pupils in KS1 use a shared cohort username & password to login.

In Year 3 and 4 pupils are given their own username and consistent password which is known by staff.

In Year 5 pupils are given an eSafety Lesson on passwords and then forced to choose their own password which is not known by anyone else and can be reset by the ICT Support Team or class teacher if needed.

14.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

14.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

You can find out data protection and other policies on our website via www.woodhouse.calderdale.sch.uk/information#gdpr-information

14.4 Access to facilities and materials

All users of the school's ICT facilities will have access rights to school systems, files and devices.

These access rights are managed by the IT Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Manager / SLT immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

14.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may not use personal devices including USB drives to store school data, or take personal data (such as pupil information) out of school.

School staff may user a personal computer to access their school email via outlook.com and Staff Drive online via onedrive.com.

15. Emerging Technologies

All new technologies will be considered and reviewed for any security vulnerabilities that may exist. This will be undertaken by suitable technical or teaching staff and reviewed by the Data Protection Officer (DPO). Suitable control measures will be adopted within school to ensure that any identified risks are managed to an acceptable level.

Emerging technologies can incorporate software and/or hardware products.

The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment. This risk is often effectively managed by ensuring software and firmware are kept updated.

When deemed necessary, staff and pupils will have appropriate awareness training regarding safe usage and any associated risk before the managed deployment of new technologies

The school will continually monitor usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate.

Methods to identify, assess and minimise risks will be reviewed regularly.

16. Filtering and Monitoring

The school has procured a filtering platform provided by Smooth Wall and hosted on site. This protection is much more sensitive and flexible to that found on home internet connections provide by domestic ISPs. In addition, pupils are supervised when using the internet in school.

The school use a common-sense approach protecting pupils from the vast majority of the most harmful content. However, no filtering system is infallible, and pupils are given clear instructions what to do if they come across content they 'don't like'. There is a robust procedure for staff to follow for any filtering failure.

In order to allow the internet to be useable there has to be some risk involved. This is managed, but there is still a risk of inappropriate content being accessed on school systems but only a small risk of harmful content being accessed.

The monitoring and reporting functionality ensures patterns of accessing or attempting to access potential harmful internet content will be identified. These patterns are more accurate than individual attempts which are most often false positives eg "Hatred & Intolerance" being a search in relation to the Romans or "Personal Weapon" being WWII related.

The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.

Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager where it is a false positive and by the Headteacher which it is a change to the filtering policy.

If users discover a website with inappropriate content, this should be logged via the ICT Helpdesk. The log will be monitored regularly by the IT Manager and reported to the headteacher where deemed necessary.

If users discover a website with potentially illegal content, this should be reported immediately to the IT Manager via ICT Helpdesk. The school will report such incidents to appropriate agencies including the local authority, CEOP or the IWF.

The school will regularly review the filtering product for its effectiveness. The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.

Any amendments to the school filtering policy will be checked and assessed prior to being released or blocked by the IT Manager in consultation with the head where a change in policy is required.

Pupils will be taught to assess content as their internet usage skills develop and will use age-appropriate tools to research internet content.

The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The school has the ability to undertake filtering when pupil devices are off-site using Smoothwall Cloud Filter. The level of access mirrors the sites allowed or denied in school. The monitoring and record keeping is limited compared to the onsite Smoothwall filtering but a significant enhancement on home broadband filtering or systems on devices supplied by the DfE and can be managed remotely.

17. Acceptable Use Policy

Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.

All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.

All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.

Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.

Any visitor who requires internet access will be asked to read and sign the relevant Acceptable Use Policy.

When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.

Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.

Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

18. Email

Staff, governors and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

Staff should not use personal email accounts during school hours or for school purposes, especially to exchange any school-related information or documents.

The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. An audit trail can be made available should this become necessary.

School email accounts should be the only account that is used for school-related business.

Staff will only use official school-provided email accounts to communicate with pupils and parents and carers, as approved by the senior leadership team and the Data Protection Officer. Most emails to parents/carers should be sent via by the school office and the Admin email address given to all parents who request an email address. This ensures a consistent approach to home school contact.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Pupils and staff will be reminded when using messaging about the need to send polite and responsible messages.

Pupils and staff will be reminded about the dangers of revealing personal information online.

Pupils must not reveal personal details of themselves or others online. Pupils should get prior permission from an adult if they arrange to meet with anyone online.

Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments. High risk attachments are flagged to the user.

All email and email attachments from external sources will be scanned for malicious content.

Pupils and staff should never open attachments from an untrusted source but should consult the IT Manager first.

Communication between staff and pupils or members of the wider school community should be professional and related to school/community matters only.

All pupils with active email accounts are expected to adhere to the generally accepted rules of netiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.

Any inappropriate use of the school messaging system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.

All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.

Pupils must immediately tell a member of staff if they receive any inappropriate message.

Irrespective of how pupils or staff access their school messages (from home or within school), school policies still apply.

Chain messages will not be permitted and should not be forwarded on.

The school requires a standard disclaimer to be attached to all external email correspondence, stating that, 'the views expressed are not necessarily those of the school'.

All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.

Email accounts should be checked regularly for new correspondence.

Purple Mash has a 2email function which imitates email but cannot be used externally. All pupils and staff have access to this and the above should apply to its use.

19. Publication of Content On-Line

Blogs/wikis/podcasts/social networking/other ways are used to publish content online to occasionally enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, staff and pupils are expected to take part in these activities in a safe and responsible manner.

20. Mobile Phone Usage in School

Mobile phones and personally-owned devices will not be used during lessons or formal school time. They should be switched off or silent at all times.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as the pool, changing rooms and toilets.

No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the head and the person or people concerned.

20.1 Pupils' use of personal devices

If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office.

If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

20.2 Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode, mobile phones or devices will not be used during teaching periods for personal messages unless permission has been granted by a member of the senior leadership team in emergency circumstances. The use of a personal mobile for Multifactor Authentication (MFA) is an acceptable use within the classroom.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose without permission.

Staff members are required to use a mobile phone for school duties, for instance in case of or emergency during off-site activities for contacting pupils or parents. Where the staff member doesn't have access to a school owned device, should they use their own devices to ring a parent, they should hide their mobile number (by inputting 141 or enabling this option in the phone settings) for confidentiality purposes.

21. Data Protection and Information Security

(To be read in accordance with the school's GDPR Documentation)

The school community will act and carry out its duty of care for the information assets it holds in line with its General Data Protection Regulation commitments.

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

The school considers the principles of the General Data Protection Regulation & Data Protection Act 2018 when creating or reviewing information-handling procedures and assessing the risks involved with handling and controlling access to all levels of information within school.

The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.

All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

All computers that are used to access sensitive information should be locked (Ctrl+Alt+Del and click Lock this computer OR ⊞+L) when unattended.

Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.

All access to information systems should be controlled via a suitably complex password.

Any access to personal and sensitive information should be assessed and granted by the DPO (Data Protection Officer) and the applicable IAO (Information Asset owner).

All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the DPO or IAO.

Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school. All office based staff likely to access and print sensitive information have been provided with local printers so documents are not left unsupervised while waiting collection.

All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, secure cloud storage, remote access over encrypted tunnel. Access to most information has been made available to staff offsite in a secure fashion where such a need has been identified.

All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

22. Management of Assets

Details of all school-owned hardware will be recorded in a hardware inventory.

All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

23. The Prevent Duty

The statutory guidance makes clear the need for schools to ensure that children are safe from radicalisation and extremist material when accessing the internet in schools. All pupil access internet is suitably filtered and monitored for misuse and reported to the DLS. See section 16 Filtering and Monitoring.

As with other online risks of harm, every member of staff needs to be aware of the risks posed by the online activity of extremist and radicalisation groups. This is covered in the mandatory safeguarding training.

24. Monitoring and Evaluation:

The school will monitor the impact of the policy and respond to issues using:

- Logs of reported incidents
- Smooth Wall monitoring logs of internet activity (including sites visited, sites blocked and search term used)
- Internal monitoring data for network activity

When appropriate, the use of surveys / questionnaires of:

- pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
- parents / carers
- staff

25. Success Criteria

All staff aware of procedures;

Incidents dealt with in line with the policy;

All staff and pupils are aware of how to be safe while using ICT and the internet inside and outside of school.

26. Equal Opportunities and Inclusion

The school is committed to working towards equality of opportunity in all aspects of school life. Our aim is to ensure that no child is discriminated against by being treated less favourably or by failure of staff to make reasonable adjustments to in recognition of pupils' needs and abilities.

27. Relationships with Other School Policies

Due to the ever-changing nature of Information and Communication Technology, this policy will be reviewed annually and reviewed by a member of the safeguarding team and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to eSafeguarding or incidents that have taken place and in relation to the aims and content of other school policies such as:
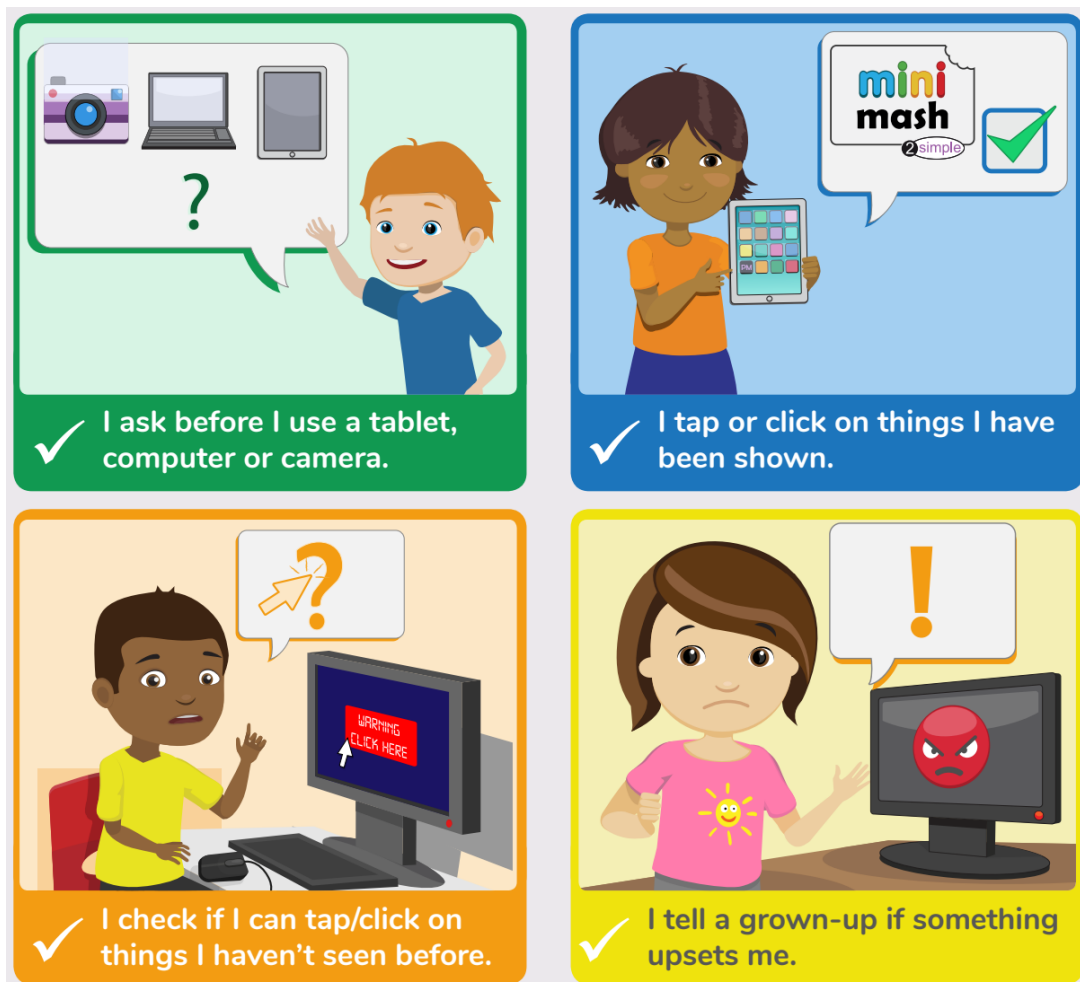
- Safeguarding and Child Protection procedure
- CPD Policy
- Inclusion Policy
- SEN Policy
- Induction Policy
- Staff Code of Conduct

Woodhouse Primary School

Acceptable use agreement for KS1

I will:

- Keep my passwords safe and never use someone else's.
- Know personal information such as my address and birthday should never be shared online.
- Know I must never communicate with strangers online.
- Always be polite when I use our school communication tools.

Signed:

Date:

Acceptable use agreement for KS2

I will:

- Only access computing equipment when a trusted adult has given me permission and is present
- Explore the online world but remember that I cannot trust everything that I see or read on the internet.
- Not deliberately look for, save or send anything that could make others upset.
- Immediately inform an adult if I see something that worries me, or I know is inappropriate.
- Keep my username and password secure; this includes not sharing it with others.
- Never share my own or others' personal information such as phone numbers, home addresses and names.
- Know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- Respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- Use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.

T = is it true?

H = is it helpful?

I = is it inspiring?

N = is it necessary?

K = is it kind?
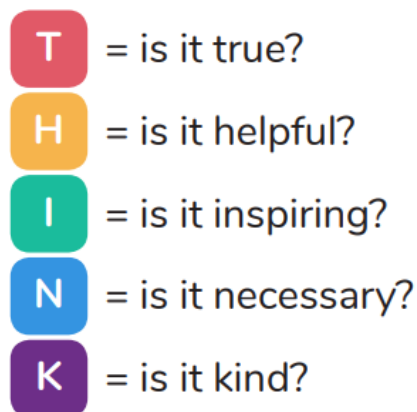
- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.
- I should follow this guidance in school or at home.

Signed: _____   Date: _____

APPENDIX 2 – Staff / Governors / Volunteer / Visitors guidelines for acceptable Computer use:

Woodhouse Primary School

**Acceptable use of the school's ICT facilities and the internet:
agreement for staff, governors, volunteers and visitors**

When using the school's ICT facilities and / or accessing the internet in school, or outside school on a work device, **I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, obscene, racist, homophobic or pornographic nature (or create, share, link to or send such material).
- knowingly view, send or receive material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress
- Use them in any way which could harm the school's equipment or reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the school community
- Access, modify or share data I'm not authorised to do so
- make statements purporting to represent Woodhouse Primary School when they are personal views
- knowingly infringe copyright or intellectual property rights
- access gambling content or use the equipment for political purposes not directly related to my job
- Promote any private business, unless that business is directly related to the school

I will:

- immediately report any illegal, inappropriate or harmful material or incident I become aware of, through the defined reporting procedure.
- let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- only use a Windows based computer on the school network (including Wi-Fi) if it is free from malware and has an up-to-date antivirus program installed and running. Free antivirus, other than Microsoft End Point Protection, is **not** sufficient.
- only access the school wireless network while signed-in on-site and understand this policy applies to any subsequent visits.
- always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

- only communicate with pupils and parents / carers and other school contacts using official school systems in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

I understand:

- that this is a brief summary of our eSafety Policy and I such check with the full policy and / or SLT should I be concerned an activity might not be considered acceptable.
- the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I must take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

Signed: _____ **Date:** _____

Name: _____ **Staff / Volunteer / Visitor / Governor**

Woodhouse Primary School

Acceptable use of the internet: agreement for parents and carers

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped and have the skills and knowledge to safely access and use digital technologies.

This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

We ask parents and carers to support us by:

- Sharing good online behaviours with your child.
- Emphasising the importance of the Acceptable Use Statements your child has agreed to.
- Highlighting the importance of accessing only age-appropriate content and sites.
- Explaining how to keep an appropriate digital footprint.
- Discussing what is and isn't appropriate to share online.
- Emphasising never to meet anyone online or trust that everyone has good intentions.
- Reporting any concerns you have whether home or school based.
- Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, please:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure
- Support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
- Ensure that images taken of pupils at school events will be for personal use only and not published (including uploaded or shared publicly via the internet)
- Refrain from using social networking sites to voice concerns regarding school issues.

APPENDIX 4 – Proforma for logging ICT / ESafeguarding incidents:

An online reporting form is provided as part of our normal ICT Incident Log. It forms a vital part of school procedures to protect staff from an innocent and explainable incident which leads to adult material being viewed on school ICT equipment. Where such material is viewed on a computer it is possible it could remain there for a significant amount of time. If discovered by a member of technical staff, or worse pupils, it would be reported and investigated. If we have a record of a genuine reason why the material is there it will protect staff from further investigation. Computers will be examined with a view to removing any offending content to prevent further incidents of this nature.

Reporting of an incident or failure of our filtering systems is not to be feared. Failing to report however, could lead to disciplinary procedures at a later stage.

Please complete the form below with as much details as possible.

- Description of what you came across: *
- Content Medium;
    - Text,
    - Image,
    - Video,
    - Audio (No need to report explicit music lyrics)
- Website address of the content
- Website address referring you too it
- If you searched and found this what search term did you use
- Please choose one: *
- Device Name: *
- Date occurred: *

APPENDIX 5 – Code of Conduct: Home learning

<div align="center">

Woodhouse Primary School

Code of Conduct : Home learning

</div>

To ensure your child's and others' safety and enjoyment of each MS Teams session, we expect parents and carers to adhere to the following:

- Ensure, to the best of your ability, that your child is punctual to ensure the smooth running of the session

- Ensure that your child is situated within a suitable communal quiet space within the home and that, where possible, background noise is kept to a minimum

- Ensure that your child is suitably dressed when operating the video function of a Teams call

- Ensure that your child, and all members of the household, use appropriate language at all times whilst the Teams session is live

- Ensure that the Teams link is not shared with anyone else

NB failure to comply with the above, and the school's positive behaviour expectations, could result in the removal of a pupil from a session.