



ONLINE SAFETY POLICY



Wood Bank School

From strong roots we grow and blossom

Policy Ratified	March 2024
Review Date	March 2026
Signed (Headteacher)	
Signed (Chair of Governors)	

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

2. Education and Curriculum

- Pupil Online Safety Curriculum
- Staff and governor training
- Parent awareness

3. Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- CCTV
- Class Dojo

5. Data Security

- Management Information System access
- Data transfer

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Visitors)

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Wood Bank School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Wood Bank School.
- 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.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Online safety is part of the [statutory safeguarding and child protection guidance](#) for schools. This includes keeping children safe from harmful and inappropriate content online as well as being able to recognise concerns and take appropriate action. In **England**, Keeping Children Safe in Education (KCSIE) is the statutory guidance for schools with the latest version in force from 1 September 2023. The KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract.) These are known as the **4 Cs of online safety**.

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed

to these risks directly. Schools should also consider how the risk from commerce applies to staff.

Scope

This policy applies to all members of Wood Bank's community (including staff, students, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Wood Bank School computing systems, both in and out of Wood Bank School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy).

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> • To take overall responsibility for online safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g., network manager) • Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents • Ensures that online safety education is embedded across the curriculum • To communicate regularly with the designated Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs •

Role	Key Responsibilities
Designated Safeguarding Leads	<ul style="list-style-type: none"> • Promotes an awareness and commitment to online safeguarding throughout the school community • Liaises with school computing technical staff • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that an online safety incident log is kept up to date • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> • sharing of personal data • access to illegal / inappropriate materials • inappropriate online contact with adults / strangers • potential or actual incidents of grooming • online bullying and use of social media
Governors	<ul style="list-style-type: none"> • To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor in their capacity as Safeguarding Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • Regular review with the Online Safety Co-ordinators (e.g., reviewing online safety incident logs, filtering / change control logs)
Curriculum Leader	<ul style="list-style-type: none"> • To oversee the delivery of the online safety element of the My Independence Curriculum • To monitor and report and concerns regarding e-safety to the Headteacher

Role	Key Responsibilities
ICT Technician (Calderdale)	<ul style="list-style-type: none"> • To report any online safety related issues that arise, to the Headteacher. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g., keeping virus protection up to date) • To ensure the security of the school IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • Schools Broadband is informed of issues relating to the filtering applied • Keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures
Teachers	<ul style="list-style-type: none"> • To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology

Role	Key Responsibilities
All Staff	<ul style="list-style-type: none"> • To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Headteacher/SLT • To maintain an awareness of current online safety issues and guidance e.g., through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils and parents should be on a professional level and only through school-based systems, never through personal mechanisms, e.g., email, text, mobile phones etc • To maintain confidentiality at all times and never share any images or content regarding pupils on any social media platform not related to the school
Parents/Carers	<ul style="list-style-type: none"> • To support the school in promoting online safety • To use the appropriate channels for complaints, not through social media platforms • To access the school website and any on-line pupil records in accordance with the relevant school Acceptable Use Agreement • To consult with the school if they have any concerns about their children's use of technology

Communication

The policy will be communicated to staff / pupils / community in the following ways:

- Policy to be posted on the school website and available in the main office
- Policy to be part of school induction pack for new staff

Handling Complaints

- The school will take all reasonable precautions to ensure online safety. 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.
- Any complaint about staff misuse is referred directly to the Headteacher.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school safeguarding procedures.

Review and Monitoring

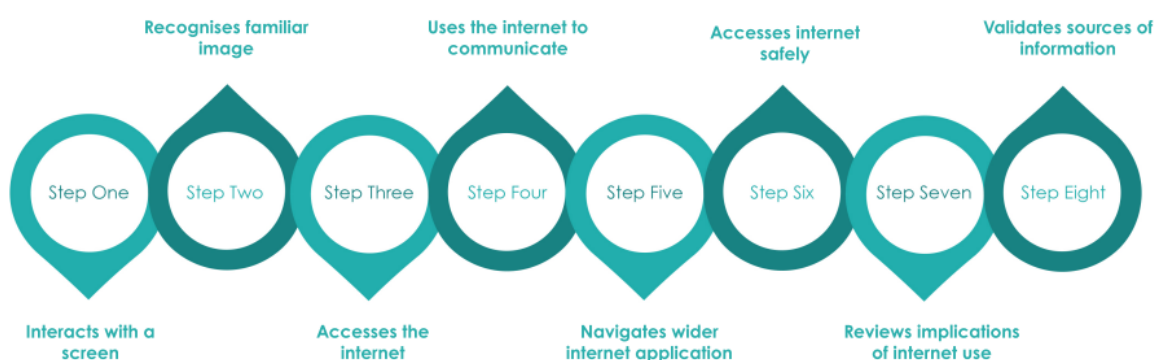
The Online Safety Policy is referenced within other school policies: Safeguarding Policy and the RSE Policy

- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online safety policy has been written by the school Headteacher and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safeguarding Policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil Online Safety Curriculum

The curriculum chain below details the steps within the Explore Curriculum that pupils follow to support them with e-safety.



Where pupils have a specific need, or it is identified across another curriculum pathway that a specific pupil requires support then a separate RSE intervention curriculum has been developed to support staff in identifying needs and plan for interventions

Staff and Governor Training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safety policy and the school's Acceptable Use Policies.

Parent Awareness and Training

This school

- Supports families through the EHC process and will discuss the dangers of the internet with parents where there are concerns
- Has a link on the school website for families that supports e-safety for pupils

3. Incident Management

Incident Management

In this school:

- There is strict monitoring and application of the Online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely a need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- Support is actively sought from other agencies as needed
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the IT and Computing Infrastructure

Internet access, security (virus protection) and filtering

Our filtering system complies with the updated guidelines issued by the Department for Education for 'Keeping Children Safe in Education 2023 (KCSIE)

Surfprotect automatically implements a default filtering policy which prevents access to the web categories detailed by the UK Safer Internet Centre, alongside a number of other inappropriate topics. This includes the following content:

- Discrimination
- Drugs/Substance abuse
- Extremism
- Gambling
- Malware/Hacking
- Pornography
- Piracy & copyright theft
- Violence
- Suicide

Network management (user access, backup)

Wood Bank

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- Has additional local network auditing software installed
- Storage of all data within the school conforms to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the [EU data protection directive](#)

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy as part of induction. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different / use the same username and password for access to our school's network
- Staff access to the schools' management information system is controlled through a separate password for data security purposes
- Provides classes with a network log-in username for pupil use
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Sets-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. [Users needing access to secure data are timed out after 5 minutes and have to re-enter their username and password to re-enter the network.]
- 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 music/media download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network
- 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
- Has limited access to drives (according to level of responsibility) set by the Headteacher
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only via an Ericom system
- 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, e.g., technical support or MIS Support, our

- Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files
 - Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
 - Uses the DfE 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 or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)
 - Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
 - Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
 - All computer equipment is installed professionally and meets health and safety standards
 - Reviews the school IT systems regularly with regard to health and safety and security.

Password Policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff to use STRONG passwords for access into our MIS system
- We require staff to change their passwords for logging on to the school network every 4 Months

E-mail

This school

- Provides staff with an email account for their professional use, LA email and makes clear personal email should be through a separate account
- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail addresses, for example admin@woodbank.calderdale.sch.uk
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language

School Website

- The Head teacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers: Head Teacher/Administration Manager and the School Administrator
- The school web site complies with the [statutory DfE 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, telephone number and we use a general email contact address: admin@woodbank.calderdale.sch.uk
- Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Learning platform

- Teachers may use virtual learning platforms to provide education for pupils unable to access on-site education
- Teachers will record all virtual lessons
- Online teaching should follow the same principles as set out in out in the school code of conduct and staff on-line safety Code of Conduct

Social Networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications
- School staff will not use their own social media to contact and student or parent and they must not share information about the school day through this platform unless preciously approved by the Headteacher

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

School use of Social Networking

The use of social media for school is to inform families and friends of what work and events the children have been taking part in, to give information about upcoming events and relevant information and to promote fun and learning for all.

Students, whilst on site, will have no access to social media whilst on school owned devices. This access is limited via proxy settings. Social media can be accessed using level 2 internet access, although it is against this policy for staff to access social media for personal reasons in school. At times however, it may be necessary to access social media for teaching and learning purposes. This is permitted, providing it is done in a secure and professional manner.

The school does have presence on some social media websites. The school uses Facebook (@woodbankschool) and their use is governed by the following rules;

- The Headteacher will delegate editorial responsibility to members of staff to ensure it is accurate and that quality of presentation is maintained
- The password is kept secured and only authorised members of staff have access.
- The account will not share anything of an unprofessional or inappropriate nature
- All inappropriate content will be logged and blocked
- Those students whose parents and carers have requested not to be featured will not be referred to or featured in any way
- Personal contact details of staff and students will not be published. The contact details provided must be those of the school office or registered school email accounts
- Content must be appropriate, necessary and will conform to all data protection, child safety and information security laws
- If there are any inappropriate comments posted or activity by parents or other persons will be dealt with in the same manner as if it was face-to-face. Any inappropriate activity by members of school staff will be dealt with in accordance with the staff code of conduct policy

CCTV

- CCTV playback will only be accessed by the Senior Leadership Team and the Premises Manager
- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the police as part of a criminal investigation
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes

Class Dojo

- We use the Class Dojo platform, which offers a social media-style interface which manages the flow of frequent information from school to home. It can be accessed through a smartphone or tablet app or through a desktop browser
- Teachers at Wood Bank will be accessing Class Dojo through school iPads or laptops
- It is secure and personal to our school and provides information in a simple format similar to Twitter and Facebook
- Class Dojo is compliant with the GDPR. Parents give permission for the school to process their child's data on the system when they complete the data processing consent form on admission
- Our Class Dojo account is only available to parents and pupils registered at Wood Bank

5. Data Security: Management Information System access and Data transfer

Strategic and Operational Practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders sign an acceptable Use agreement form. We have a system so we know who has signed.
 - o staff,
 - o governors,
 - o pupils
 - o parentsThis makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Mobile [phones must be kept in lockers or locked in the cupboards
- Staff members may use their phones during school break times but only in the staff room
- All visitors are requested to keep their phones on silent and may not use them in a classroom
- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Staff may use their phones during break times. If a staff member is expecting a personal call, they must speak to SLT to receive permission for them to be used.
- Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g., changing rooms and toilets.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Pupils' use of personal devices

- No pupils should bring his or her mobile phone or personally owned device into school. Any device brought into school will be confiscated.

Digital images and video

In this school:

- We gain parental/carer 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.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- 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.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant 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 equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, 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 equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.



Staff Online Safety Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are required to sign this code of conduct. Members of staff must consult the schools Online Safety policy for further information and clarification.

- All internet activity must be appropriate to staff professional activity or the pupil's education.
- Access must only be made via the authorised accounts and passwords, which must not be made available to any other person under any circumstances. This would be considered a disciplinary matter open to serious sanctions.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is excluded.
- The downloading or installation of software/hardware is not allowed.
- All data travelling offsite must be stored on encrypted laptops or USB pens provided by the school.
- Staff must not use personal equipment to record photographs or video of pupils.
- Staff must only use personal mobile phones to conduct authorised school business. Where possible, staff must use the school landline or the school mobile phone available from the office.
- Online safety guidelines must be followed at all times and staff have a duty to report any instances related to cyber-bullying or child protection to the appropriate member of staff.
- Staff must only use authorised school email accounts when conducting school business. The use of personal email accounts for this purpose is prohibited.
- Staff must uphold a high level of professional language and content when using the school email system. Views expressed in emails can be seen to represent those of the school and/or the LA, and so staff must converse accordingly.
- Staff must be professional in all modes of online activity. This includes the use of social networking sites outside of school hours. Staff must adhere to the guidelines outlined on the reverse of this policy.
- Use for personal gain, gambling, gossip, libel, political purposes or advertising is excluded.
- You must not knowingly send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- Copyright of materials and intellectual property rights must be respected.
- Violation of the above Code of Conduct will result in Sanction procedures outlined in the Online Safety and Disciplinary Policies.

Guidelines for Wood Bank Staff regarding the use of Social Networking Sites

- Facebook and other social networking sites are now part of everyday life and represent new and innovative ways to communicate. As professionals who work with young people, we must take extra care when using these sites in order to safeguard ourselves, our pupils and our school.
- Situations can, and have, become quickly out of hand after personal information was obtained online. Allegations made about online conduct which directly compromise the professional standing of a member of staff can lead to disciplinary action, dismissal or further legal action.
- Wood Bank staff are therefore required to uphold their professional reputation, and that of the school, when using social networking websites and the internet. In order to protect themselves against false allegations and misinterpretations, it is highly recommended that colleagues adhere to the following guidelines:

Safeguarding the School and its Students

- Staff must remember that although they are out of school, their activities online may be interpreted as actions or views of the school as a whole.
- Staff must never discuss school matters or disclose information about pupils and staff on social networking websites. This includes "status updates" which may insinuate things about the school.
- Staff must not disclose that they are employed by Wood Bank School.
- Staff must not, under any circumstances, upload any videos or photographs of pupils, staff or activities at Wood Bank School onto social networking websites. This constitutes a serious breach of trust and professional responsibility.

Safeguarding Yourself

- Staff must safeguard themselves by ensuring that the correct privacy settings are in place to restrict access to personal information.
- Where possible avoid uploading, or being featured in, photographs which may be deemed inappropriate. This includes nudity, being under the influence of alcohol, or being photographed with a known criminal or sex offender.
- Do not join or condone any groups or activities which represent a controversial, illegal, or inappropriate message.
- Do not say or do anything online that you would not be happy to say in person.

Declaration

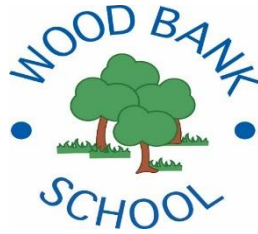
I have read and understood the "Staff Online Safety Code of Conduct". I have also read and understood the "Guidelines for Wood Bank Staff regarding the use of Social Networking Sites" and agree to maintain a professional level of conduct when using social networking websites and the Internet. I understand that a breach of these guidelines may result in disciplinary or legal actions being taken against me.

Full Name: _____

Position: _____

Signed: _____

Date: _____



Wood Bank Online Safety Code of Conduct (Volunteers and Work Placements)

To ensure that you are fully aware of your responsibilities when using information systems and when communicating with pupils, you are required to sign this code of conduct. You may consult the Online Safety policy for further clarification and information. Copies are available on request

- All Internet activity must be appropriate and aimed to further the education of Wood Bank pupils.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is excluded.
- The downloading or installation of software/hardware is not allowed.
- You must not, under any circumstances, remove data belonging to Wood Bank from the School network.
- You are forbidden from using personal equipment to record photographs or video of pupils. You may be asked to use equipment belonging to the school for assessment purposes, and may do so under the supervision of Wood Bank staff.
- The use of mobile phones during lessons is not allowed. Use is restricted to break and lunchtimes, and to be used in designated 'mobile use free' areas.
- Online safety guidelines must be followed at all times and you have a duty to report any instances related to cyber-bullying or child protection to an appropriate member of staff.
- You must be professional in all modes of online activity. This includes the use of social networking sites outside of school hours.
- Use for personal gain, gambling, gossip, libel, political purposes or advertising is excluded.
- You must not knowingly send, receive or view any material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- Copyright of materials and intellectual property rights must be respected.

Violation of the above Code of Conduct will result in Sanction procedures outlined in the Online Safety Policy, and may result in the suspension or termination of your placement at Wood Bank. In more severe cases, legal action may be sought.

Full Name: _____

Date: _____