WOOD BANK SCHOOL

ONLINE SAFETY POLICY

Policy Ratification	**October 2017**
Review Date	**October 2018**
Signed (Headteacher)	
Signed (Chair of Governors)	

Contents

1. Introduction and Overview

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

2. Education and Curriculum

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

3. Expected Conduct and 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
- Video Conferencing

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 (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to Online safety incidents, handling infringements
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE

1. Introduction and Overview

Equality Statement

At Wood Bank School we intend to provide a safe, secure, caring environment where everyone is valued and respected equally. We aim to provide an inclusive education where children develop independent learning skills and are taught according to need whatever their age, gender, background, beliefs or abilities. National legislation re disabilities, race relations and special education needs underpin this policy, which has also taken into consideration national, local and school policies on Special Educational Needs, Gifted and Talented, Equal Opportunities and Health and Safety.

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.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, substance abuse, hate sites, lifestyle website promoting eg pro-anorexia, self-harm, suicide
- Ignoring age ratings in games (exposure to violence associated with often racist language)
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Online bullying in all forms
- Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming)

- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Extremism
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope (from Yorkshire & Humber Grid for Learning)
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	• 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 receive regular Online monitoring reports from ICT Manager • 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)

Role	Key Responsibilities

Designated Safeguarding Leads	• Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies/documents
	• Promotes an awareness and commitment to Online safeguarding throughout the school community
	• ensures that Online safety education is embedded across the curriculum
	• liaises with school computing technical staff
	• To communicate regularly with SLT and the designated Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
	• 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:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • Online bullying and use of social media

Governors	• 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 • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinators of eg Online safety incident logs, filtering / change control logs)
Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinators regularly

Role	Key Responsibilities
ICT Technician	• To report any online safety related issues that arise, to the Head Teacher. • 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 • The school's policy on web filtering is applied and updated on a regular basis • YHGFL is informed of issues relating to the filtering applied by the Grid • 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 • Educating Parents/Carers and raising awareness as instructed by Headteacher through training and information sharing
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Nominated contact(s)	• To ensure all YHGFL and Calderdale MBC ICT services are managed on behalf of the school including maintaining the YHGFL database of access accounts
Teachers	• 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 (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws, where appropriate

Role	Key Responsibilities
All Staff	• 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 online safety coordinators • 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 should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking/use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies

Role	Key Responsibilities
Parents/Carers	• To support the school in promoting online safety by reading and signing the Acceptable Use Agreement which includes the pupils' use of the Internet • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • 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
External Groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication

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

- Policy to be posted on the school website, available in staffroom policies folder and individual copies distributed to all staff
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year where children are cognitively able to understand this given Wood Bank caters from children with Profound, Multiple and Severe Learning Difficulties
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

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

  - Interview/counselling by Class Teacher/Headteacher
  - Informing parents or carers;
  - Removal of Internet or computer access for a period.
  - Referral to LA / Police.

- Our ICT Technician acts as first point of contact for any complaint. Any complaint about staff misuse is referred 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 school / LA Child Protection procedures.

Review and Monitoring

The Online safety policy is referenced within other school policies: Child Protection Policy, Anti-Bullying Policy, Behaviour Policy

- The school has an ICT Technician who will be responsible for document ownership, review and updates.
- 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

This school has a clear, progressive Online Safety education programme as part of the Safeguarding curriculum. It is built on LA/YHGfL online safeguarding and online literacy framework for EYFS to Y6/ National Guidance. This covers a range of skills and behaviours appropriate to their age, experience and cognitive capacity including (where appropriate)

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - To know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
    - To understand why they must not post pictures or videos of others without their permission
    - To know not to download any files – such as music files - without permission
    - To have strategies for dealing with receipt of inappropriate materials
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons
    - To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying
    - To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies,

i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming / gambling

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-safeguarding policy and the school's Acceptable Use Policies.

Parent Awareness and Training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and 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 online bullying

Staff

- are responsible for reading the school's Online safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online safety acceptable use agreement form at the time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

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 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 (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- 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

This school:

- Has the educational filtered secure broadband connectivity through the YHGfL and so connects to the 'private' National Education Network;
- Uses the YHGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from YHGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or YHGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network.
- Only unblocks other external social networking sites for specific purposes.
- Has blocked pupil access to music download or shopping sites – Ebay etc
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the YHGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's website.
- Requires staff to preview websites before use [where not previously viewed or cached] Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search etc
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to Calderdale MBC ICT. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or Calderdale ICT Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with YHGfL & Calderdale ICT services and policies / requires the Technical Support Provider to be up-to-date with YHGfL services and policies;
- Storage of all data within the school will conform 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 where storage is hosted within the EU.

To ensure the network is used safely, this school:

Ensures staff read and sign that they have understood the school's Online safety Policy. 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;

We provide pupils with a network log-in username

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;

Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

Requires all users to always log off when they have finished working or are leaving the computer unattended;

Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [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 all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;

Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional

responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
Maintains equipment to ensure Health and Safety is followed;
e.g. projector filters cleaned by ICT manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
e.g. teachers access report writing module; SEN coordinator - SEN data;
Ensures that access to the school’s network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / 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@Wood Bank.calderdale.sch.uk
- Will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- 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 YHGFL-provided 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.

Pupils

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

Staff

- Staff can only use the LA email systems on the school system
- Staff only use LA e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School Website

- The Headteacher 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/ICT Manager/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;
- We expect teachers using' school approved blogs to password protect them and run from the school website.

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 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.

CCTV

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.

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

Strategic and Operational Practices

At this school:

The Head Teacher 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 where data protection may have been compromised.
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.

- staff,
- governors,
- pupils
- parents

This 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.
We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution (ERICOM) so staff can access sensitive and other data from home, without need to take data home.
School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

Staff have secure area(s) on the network to store sensitive documents or photographs.
We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
We use encrypted flash drives if any member of staff has to take any sensitive information off site.

We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
All servers are in lockable locations and managed by DBS-checked staff.
We use Calderdale MBC remote secure back-up network / admin, curriculum server.
We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and <get a certificate of secure deletion for any server that once contained personal data.
Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
Paper based sensitive information is shredded, using cross cut shredder.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.
- 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.
- Staff members may use their phones during school break times.
  All visitors are requested to keep their phones on silent.
- 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 mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times through the Headteacher
- Mobile phones and personally-owned devices will not be used in any way 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 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.

- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

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.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number.
- 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.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141 or 1470) their own mobile number for confidentiality purposes.

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 safe-guard 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: _____

Dear Parent/Carer,

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Wood Bank School provides supervised access to the Internet. We believe that the use of the Web and e-mail is worthwhile and an essential tool for children as they grow up in the modern world. Please would you read the rules for responsible Internet use and sign and return the consent slip so that your child may use the Internet at school.

Our Internet service provider Schools Broadband filters any unsuitable sites containing inappropriate language and images. It is also able to decode sites which may try to 'hide' its content.

We believe that vigilance on behalf of the staff is the main step to ensuring no unsuitable material is accessed. The children will be supervised at all times and advised of the sites they should visit. Sites chosen by teachers to use as the basis of a lesson will have been checked beforehand.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to not access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be held liable under any circumstances for any damages arising from your child's use of the internet facilities.

Please complete, sign and return the slip on the following page. Your child will be unable to use the Internet independently until we receive the form.

Yours sincerely

Richard Pawson
Headteacher

Acceptable Use Agreement

I understand that where it is considered ***appropriate*** *ie- full comprehension is possible, that the school will discuss the Acceptable Use of the internet with my child and that they will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that my child will be safe when they use the internet and systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy, details on which can be found in the Online Safety Policy published on the Wood Bank School website www.woodbank.calderdale.sch.uk

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Pupil Name: _____

Relationship to Pupil: _____

Signed: _____

Date: _____