ICT and Online Safety Policy

Policy updated by:	A.Earl
Reviewed by staff:	December 2024
Review due:	December 2025
Agreed by Headteacher:	M. Hance

ICT & ONLINE SAFETY POLICY

POLICY STATEMENT

New Horizons Academy is committed to the creation and continual maintenance of a safe ICT and learning environment.

This policy identifies the essential elements of our school wide approach towards current and emerging technologies within all our schools and more importantly how our children and staffs' relationship operates with those technologies. Educating our children and staff to have safe behaviours whilst being able to maximise the learning opportunities these technologies offer is key for all to thrive in the digital world.

We expect staff, pupils, visitors, contractors, and other employers to share this commitment by complying with our policies and procedures and to understand that they also have a legal and moral obligation to themselves and to others.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying, or other e-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.

New Horizons Academy 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 e-safety behaviour that take place out of school.

We believe that good technology management is an important and integral part of all employee's responsibility. The avoidance of significant risk to the safety of our children when they are online is a priority.

To do this effectively we will take a systematic approach to identifying risks and ensuring that resources are allocated proportionally to manage them. The school examines their own technology activities and makes suitable and sufficient assessments of any risks. These assessments will determine school priorities and set objectives for eliminating hazards, reducing risks and achieving a progressive and safe approach to technology management, usage and control.

Online safety places a responsibility on all staff to take reasonable care of their own safety and the safety of others.

It is the aim of the school and local governing body, 'To provide a safe working and learning environment for staff, pupils and visitors'.

The arrangements outlined in this Policy and the various other technology procedures cannot prevent accidents occurring but do aim to foster a "no blame culture" so that children and staff are able to report anything of concern to senior staff. However, the senior leaders within each school will take all reasonable steps to identify and reduce hazards within its control to a minimum.

All staff and pupils must appreciate that their own safety depends on their individual conduct and vigilance whilst on line or on school premises or whilst taking part in school-sponsored activities.

ORGANISATION

Day-to-day running of school technologies is delegated to the Headteacher and school management team. They have a responsibility in making sure all risks are managed effectively on site. Sensible and effective management of IT technologies and systems relies on every member of the school management team making sure risk is managed responsibly and proportionately.

NEW HORIZONS ACADEMY

As the employer, the school is responsible for making sure that risks, particularly the risks to staff and pupils, are managed so far as is reasonably practicable. IT functions are delegated to members of staff within the school to fulfil on behalf of the employer.

As the employer New Horizons Academy will:

- Put in place sensible approaches to IT technologies, with clear policies that focus on the real risks.
- Implement arrangements that manage the risks to staff, pupils and visitors who may be affected by school activities.
- Tell employees about the real and significant risks in the school and the precautions they need to take to manage them.
- Make sure employees have the relevant information and training to manage risks on a day to day basis, including access to competent IT advice.
- Check that control measures have been implemented and remain appropriate and effective.

THE GOVERNORS

- Take reasonable steps to make sure that the school is following the employer's policy and procedures
  e.g. through regular discussion at governance meetings.
- Ensure staff receive adequate training to enable them to carry out their responsibilities.
- Promote a sensible approach to online safety, making use of competent IT advice when required.
- Work in close partnership with the Headteacher and senior management team to support sensible IT management and to challenge as appropriate.

HEADTEACHER

Headteachers and the school management team have considerable autonomy in the day-to-day running of their schools. It is important that they exercise this autonomy in line with the schools policies, procedures and standards.

The Headteacher must:

- Ensure that the school is following the ICT and Online Safety Policy and has effective arrangements for managing the real online risks at the school.
- Maintain effective communications with employers, governors, and the school workforce, and give clear information to pupils and visitors, including contractors, regarding the ICT risks.

- Make sure that staff have the appropriate training and competencies to deal with risks in their areas of responsibility.
- Make sure that staff understand their responsibilities and know how to access support and advice to help them manage risks responsibly.

ONLINE SAFETY LEAD:

Though the Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, the day-to-day responsibility for e-safety will be delegated to the Designated Safeguarding Lead.
They will.

- Lead on online safety issues.
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice for staff.
- Liaise with school technical staff.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Meet regularly with the online safety Governor to discuss current issues, review incident logs.
- Report regularly to the Senior Leadership Team.
- Ensure the school meets required online safety technical requirements and any Local Authority/other relevant body online safety Policy/Guidance that may apply.
- Keep up to date with online safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

DESIGNATED SAFEGUARDING LEAD

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- Cyber-bullying

OTHER SCHOOL LEADERS

The IT Services Manager, Business Manager and or, the IT contractor often take on the lead for IT technologies on site. They often provide the focal point for the school's IT management arrangements. Their school wide roles may include:

- Management and monitoring of purchasing IT technologies.
- Advising contractors of current IT issues and overseeing their activities on site.
- Ensuring staff and visitors are aware of IT procedures and the precautions to follow reporting on anything of concern.
- Implementation, monitoring and review of training procedures.
- Preparation of reports and returns for the school leadership team.

STAFF

All staff play an important part in using IT technologies appropriately. All staff need to ensure that they possess the skills and knowledge to teach children and parents about keeping safe online. An educational approach to technologies is vital to enable children and adults to thrive in the digital world. Being a critical thinker is the greatest asset a teacher can impart on a child to enable them to maximise their usage of technologies.

Staff must:

- Ensure that pupils internet access is monitored at all times and that no child is left unattended while using the internet.
- Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, guide students to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Take reasonable care for their online safety and that of others who may be affected by their actions.
- Be familiar with the schools ICT and online policy
- Ensure IT, rules, routines and procedures are being applied effectively by both staff and pupils.
- Cooperate with the Headteacher, fellow members of staff, contractors and others to enable them to make and keep safe.
- Raise IT and online safety concerns in line with local arrangements.
- Be familiar with cyberbullying and bring concerns to the DSL
- Know how to respond to incidents of concern e.g. “youth produced sexual imagery, indecent images, inappropriate searches, “Prevent” related issues.
- Ensure online safety issues are embedded in all aspects of the curriculum and other activities.

PUPILS

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- 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.

PARENTS & CARERS

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, websites and information

about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

HIRERS, CONTRACTORS AND OTHERS

- When the premises are used for purposes not under the direction of the Headteacher then the person in charge of the activities for which the premises are in use will ensure that they make no attempt to use the schools IT systems.
- The Headteacher, via the Business Manager and the Site Manager / Caretaker, will seek to ensure that hirers, contractors and others are unable to access school IT systems. This means that all systems are either locked away or have strong password protection.

ONLINE SAFETY TEAM

New Horizons Academy has an online safety team that includes different members of staff (DSL,Advocates, teachers, IT Services Manager). The online safety team will:

- Promote and raise awareness of keeping safe online with all stakeholders.
- Gain a representation of views from all stakeholders and take action to make improvements to our online safety offer.
- Provide additional training and support to staff.
- Provide support for parents and carers.
- Monitor and evaluate the effectiveness of online safety education.
- Liaise with external agencies to provide additional support.

RISK ASSESSMENT

- The Senior Management Team will ensure that risk assessment of IT technology systems are undertaken and compliance with statutory obligations within individual schools, audits and inspections are carried out from time to time.

REVIEW

- The school will review this policy statement from time to time and update, modify or amend it as it considers necessary to ensure the health, safety and welfare of staff and students. This review will be a minimum of every two years and after any serious accident.

SCHOOL NETWORKS, EQUIPMENT AND DATA SAFETY

The purpose of this Section is to give schools an understanding of the principles, which should be followed in the setting up networks, purchasing and managing equipment and data safety.

All new employees will be shown all the IT procedures during their induction period. Schools must ensure that all staff are aware of data protection protocols, online safety training, equipment storage and network monitoring procedures as soon as practicable. Within this policy the term network relates to both a schools physical windows network and the schools G Suite For Education system.

SCHOOL NETWORKS

TECHNICAL AND INFRASTRUCTURE APPROACHES

New Horizons Academy will:

- Have filtered secure broadband connectivity.
- Use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Ensure network health through use of anti-virus software.
- Use individual, audited logins where age appropriate.
- Use DfE approved systems such as S2S, secured email to send personal data over the internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site.
- Block all chat and social networking sites except those that are part of an educational network, approved Learning Platform or valid CPD opportunities.
- Only unblock other external social networking sites for specific purposes that relate to Teaching & Learning or for communicating with parents and the wider school community.
- Only use an approved service for video conferencing activity.
- Block access to music download or shopping sites – except those approved for educational purposes such as Audio Network.
- Provide staff with an email account for their professional use and make clear personal use of this email account is not allowed.
- Will only allow guest devices to connect to a dedicated Wifi network for internet access and not the main network.
- Will ensure 2 Form Authentication is implemented to sure systems when available.

USING THE SCHOOL NETWORK, EQUIPMENT AND DATA SAFETY

The computer system / network is owned by New Horizons Academy and is made available to staff and pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

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

To ensure the network is used safely, New Horizons Academy will:

- Ensure staff read and sign that they have understood the school's IT Online Safety Policy. Following this, they are set-up with internet, email access and network access.
- All pupils have their own unique username and password which gives them access to the school network.
- Pupils must not be allowed to use devices without suitable supervision by a member of staff.
- 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.

- 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 lock if they 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.
- 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. Under no circumstances should equipment be used by family members or for personal use. e.g storage of personal photos/video, personal email, games, social networks, streaming services.
- Maintains equipment to ensure Health and Safety is followed, e.g. projector filters cleaned by I.T. staff. Equipment installed and checked by approved suppliers/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.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password.
- Makes clear responsibilities for the daily backup of MIS and finance systems and other important files.
- 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.
- All our wireless networks must be secured to industry standards appropriate for educational use.
- All computer equipment is installed professionally and meets health and safety standards.

DIGITAL VIDEO, IMAGES, WEB SITE, LEARNING PLATFORMS AND

CCTV SYSTEMS

The purpose of this Section is to give schools an understanding of the principles, which should be followed in the managing digital videos, images and CCTV systems and data safety.

USE OF DIGITAL VIDEO AND IMAGES

New Horizons Academy will.

- 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.
- Ensure relevant staff are made aware of any pupil whose parent has withheld consent
- Digital images / videos must only be taken with school equipment. All images to be deleted from camera memory cards as soon as it has been transferred to the network.

- Digital images / videos of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- A record is kept to show staff have read and understood the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- Pupils are taught about how images can be manipulated in their Online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- 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, including from peers.

WEBSITES

- The Headteacher takes overall editorial 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.
- Most material is the school's own work - where other's work is published or linked we credit the source(s) used and state clearly the author's identity or status.
- The point of contact on the web site is the school address / telephone number - we use a general email contact address rather than for a specific person.
- Home information or individual email 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 or wikis to password protect them.

LEARNING PLATFORMS

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the school platform will only be accessible by members of the school community.
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform.
- 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' Learning Platform for such communications.

CCTV

- CCTV may be used for the purpose of protecting the safety of staff, students and visitors and to help secure the physical premises. Notices of recording including details of the Data Controller and where a copy of this policy can be obtained will be included on clearly visible signs posted at all entrances to the school site(s).
- All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.

- Where the school instals new CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

SAFETY PROTOCOLS

The purpose of this Section is to give schools an understanding of the principles of how staff and children should behave to maintain data safety in the digital world.

DIGITAL SECURITY

Within the school:

- The use of portable USB Pen / Flash Drives and Portable Hard Drives is strictly prohibited. Exception being for when used by IT Support for troubleshooting and other network admin tasks.
- Staff who have access to confidential data will have 2 Form Authentication enabled when available.
- All staff and governors are DBS checked and records are held in one central record.
- New Horizons Academy requires staff to use strong passwords for access into all systems.
- Staff have a secure area on the network to store sensitive documents or photographs.
- New Horizons Academy requires staff to log-out or lock systems when leaving their computer, but also enforce an idle time lock-out. (timeouts in classrooms may differ due to a teacher delivering lessons)
- Staff know who to report any incidents where data protection may have been compromised.
- New Horizons Academy requires that any Protect and Restricted material must be encrypted if the material is to be removed from the school. We limit such data removal but in the event that data can not be transferred any other way devices must be encrypted.
- Staff use the DfE S2S site to securely transfer CTF pupil data to other schools.
- Staff store any Protect and Restricted material that is in an un-encrypted format (such as paper) in lockable storage cabinets in a lockable storage area.
- All servers are managed by CRB/DBS-checked staff.
- Staff are to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- New Horizons Academy must use a recognised confidential disposal company for disposal of system hard drives where any protected or restricted data has been held.
- 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 a cross cut shredder.

PROTECTIVE MARKING LEVELS

The combined force of the Data Protection Act and Data Handling Procedures in Government make it critical to recognise the sensitive personal data held and to protect and secure personal data. To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of information and information systems, and provide comparable levels of information protection when the data is shared, the Government Protective Marking Scheme is used to indicate the sensitivity of data. This comprises five markings. In descending order of sensitivity they are:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- PROTECT

Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

Most Learner or staff personal data that is used within schools comes under the PROTECT classification.

CRITERIA FOR ASSESSING PROTECT ASSETS:

- cause distress to individuals.
- cause risk to the school.
- breach proper undertakings to maintain the confidence of information provided by third parties.
- breach statutory restrictions on the disclosure of information
- cause financial loss or loss of earning potential, or to facilitate improper gain.
- unfair advantage for individuals or companies.
- prejudice the investigation or facilitate the commission of crime.
- disadvantage government in commercial or policy negotiations with others.

CRITERIA FOR ASSESSING RESTRICTED ASSETS:

- affect diplomatic relations adversely.
- cause substantial distress to individuals.
- make it more difficult to maintain the operational effectiveness or security of the United Kingdom or allied forces.
- cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies.
- prejudice the investigation or facilitate the commission of crime.
- breach proper undertakings to maintain the confidence of information provided by third parties.
- impede the effective development or operation of government policies.
- to breach statutory restrictions on disclosure of information.
- disadvantage government in commercial or policy negotiations with others.
- undermine the proper management of the public sector and its operations.

CRITERIA FOR ASSESSING CONFIDENTIAL ASSETS:

- materially damage diplomatic relations (i.e. cause formal protest or other sanction).
- prejudice individual security or liberty.
- cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations.
- work substantially against national finances or economic and commercial interests.
- substantially to undermine the financial viability of major organisations.
- impede the investigation or facilitate the commission of serious crime.
- impede seriously the development or operation of major government policies.
- shut down or otherwise substantially disrupt significant national operations.

WHAT MEASURES SHOULD SCHOOLS TAKE?

It is a legal requirement to protect sensitive data, and Data Handling Procedures in Government sets out the measures that the school should adopt to maintain data security:

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- For schools, this means that they must encrypt any data that is classified as Protect (or higher) if this data is removed or accessed from outside any approved secure space such as a school office. Education organisations must also ensure that data classified as Protect or higher is encrypted when it is in transit from one location to another, including transit from one approved secure location to another.

Summary of the Dos and Don'ts
DATA SECURITY

Passwords - Do

- use a strong password (strong passwords require a minimum of eight characters and contain upper and lower case letters, as well as numbers and symbols. The use of a paraphrase is encouraged)

Passwords - Don't

- never share your passwords with anyone else or write your passwords down (on post-its, diaries)

- save passwords in web browsers of shared computers if offered to do so

Laptops - Do

- prevent people from watching you enter passwords or view sensitive information

- log-off / lock your 'desktop' when leaving your PC or laptop unattended.

Sending and sharing - Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner(s) if you are not sure.
- ensure 'Protected' data is encrypted before sending to outside agencies.

Sending and sharing - Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives)
- send sensitive information by email unless it is encrypted. Pupil data must be sent via S2S (DFE secure web site)

Working on-site - Do

- lock sensitive information away when left unattended, i.e. in lockable drawers, log off or lock workstation

Working on site - Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site - Do

- wherever possible access data remotely instead of taking it off-site - using approved secure authentication
- make sure you sign out completely from any services you have used

SOCIAL MEDIA

The purpose of this Section is to give an understanding of the principles, which should be followed in the managing of social media.

INTRODUCTION

- The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter and maintaining pages on internet encyclopaedias such as Wikipedia.
- While recognising the benefits of these media for new opportunities for communication, this guidance sets out the principles that all staff and contractors are expected to follow when using social media.
- It is crucial that pupils, parents and the public at large have confidence in the schools decisions and services. The principles set out in this guidance are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school are safeguarded.
- Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

SCOPE

- This guidance applies to all staff, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this guidance.

- This guidance covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of each school. Only designated staff are allowed to post on school media sites.
- This guidance applies to personal webspace such as social networking sites (for example Facebook, Twitter, Instagram, WhatsApp), blogs, chatrooms, Forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this guidance must be followed irrespective of the medium.

LEGAL FRAMEWORK

- New Horizons Academy is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including: The Human Rights Act 1998Common law duty of confidentiality, and the Data Protection Act 1998.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

New Horizons Academy could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyber-bullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the school liable to the injured party.

RELATED POLICIES AND GUIDANCE

- Safeguarding and Child Protection Policy
- Staff Code of Conduct

New Horizons Academy staff will always be: professional, responsible and respectful. You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.

You must not engage in activities involving social media which might bring the school into disrepute.

You must not represent your personal views as those of the school on any social medium.

You must not discuss personal information about pupils, the school or school staff and other professionals you interact with as part of your job on social media.

You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or the school.

You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school.

PERSONAL USE OF SOCIAL MEDIA

Staff members must not explicitly identify themselves as employees of the school or service providers for the school in their personal webspace. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Staff members must not have contact through any personal social medium with any pupil, whether from the school or any other school, unless the pupils are family members.

The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

Staff members must not have any contact with pupils or pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity or suitability.

Staff members must decline 'friend requests' from pupils and parents of pupils they receive in their personal social media accounts.

On leaving the school service, staff members must not contact the school pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former school by means of personal social media.

Information staff members have access to as part of their employment, to personal information about pupils and their family members, colleagues, and other parties and school must not be discussed on their personal webspace.

Photographs, videos or any other types of images of pupils and their families or images depicting staff members wearing school uniforms or clothing with school logos or images identifying sensitive school premises (eg care homes, secure units) must not be published on personal webspace.

The school email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

The school corporate, service or team logos or brands must not be used or published on personal webspace.

The school permits limited personal use of social media while at work. Access to social media for educational research / CPD is permitted.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the workplace.
Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online. it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

USING SOCIAL MEDIA ON BEHALF OF THE SCHOOL

Staff members can only use official school sites for communicating with pupils or to enable pupils to communicate with one another.

There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage. Central approval must be sought.

Official school sites must be created only with the approval of the Headteacher. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

MONITORING OF INTERNET USE

New Horizons Academy will monitor usage of its internet and email services without prior notification or authorisation from users.

Users of email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's IT system.

BREACHES OF THE GUIDANCE

Any breach of this guidance may lead to disciplinary action being taken against the Staff member/s involved in line with New Horizons Academy Guidance and Procedure.

A breach of this guidance leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school liable to third parties may result in disciplinary action or dismissal.

Contracted providers must inform the school immediately of any breaches of this guidance so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school.

Any action against breaches should be according to contractors' internal disciplinary procedures.

EDUCATION AND TRAINING

The purpose of this section is to give an understanding of the principles of how staff and children should be educated in the usage, staying safe and ensuring that both staff and children are able to report when they are uncomfortable with what they are seeing and hearing on the range of technologies available to them.

STAFF

- Staff should be made aware that internet use is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff should also be advised that any use of the internet for purposes which are illegal or which may bring the profession into disrepute (such as viewing online images of children, inciting racial hatred, etc) will lead to disciplinary and, where necessary, criminal action. This applies to conduct both in and outside the work environment.
- Filtering systems will be managed by senior members of management staff and have clear procedures for reporting any concerns.

- According to Keeping Children Safe in Education, our systems and training must enable us to identify individual children who may be at risk. Our procedures should ensure that everyone knows what to do next to protect them.
- The schools filtering solution will email alerts to designated members of the safeguarding team in relation to attempted access to blocked sites, both at the time of access and in regular reports.
- Staff training in safe and responsible internet use and on the school Online safety Policy will be provided and updated annually.
- All new staff should receive safeguarding training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

GOVERNORS

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

COMPLAINTS, ALLEGATIONS AND INFRINGEMENTS

The purpose of this Section is to give an understanding of the principles of how staff and children deal with complaints, allegations and infringements.

COMPLAINTS

New Horizons Academy 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. New Horizons Academy can not accept liability for material accessed, or any consequences of internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Any complaint should be referred to the Headteacher.

ALLEGATIONS

It is essential that any allegation made against a teacher or other member of staff or volunteer is dealt with fairly, quickly, and consistently.

CYBER BULLYING

Complaints about cyber-bullying are dealt with in accordance with our Anti-Bullying Policy and, where necessary, Safeguarding Procedures.

Everyone should minimise the potential for and be aware of the impact of cyber-bullying, which might include:

- Sending threatening or disturbing text messages.
- Homophobia, racism or sexism.
- Making silent, hoax or abusive calls.
- Creating and sharing embarrassing images or videos.
- 'Trolling', the sending of menacing or upsetting messages on social networks, chat rooms or online games.
- Excluding children from online games, activities or friendship groups.
- Setting up hate sites or groups about a particular child.
- Encouraging young people to self-harm.
- Voting for someone in an abusive poll.
- Hijacking or stealing online identities to embarrass a young person or cause trouble using their name.
- Sexting - which may be done to pressure a child into sending images or engaging in other unsafe and / or inappropriate activity.

We adopt a zero-tolerance approach to all forms of bullying behaviour and expect pupils and parents to do the same. Any concerns about online or cyber-bullying should be reported to the school Designated Safeguarding Lead without delay.

INFRINGEMENTS

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school and will reflect the school's disciplinary procedures.

WHERE AN ALLEGATION IS MADE AGAINST A MEMBER OF STAFF

Keeping Children Safe in Education (Part four) defines an allegation as :

"... all cases in which it is alleged that a teacher or member of staff (including volunteers) in a school or college that provides education for children under 18 years of age has:

- behaved in a way that has harmed a child, or may have harmed a child.
- possibly committed a criminal offence against or related to a child. or
- behaved towards a child or children in a way that indicates he or she would pose a risk of harm to children.

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

APPROPRIATE AND INAPPROPRIATE USE BY CHILDREN OR YOUNG PEOPLE

This policy details how children are expected to use the internet and other technologies within the school, including downloading or printing of any materials. This policy should allow children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an email to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

New Horizons Academy will encourage parents and carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreement is accepted by the child or young person with the support of the parent or carer. This is also intended to provide support and information to parents and carers when children and young people may be using the internet beyond the school setting or other establishment.

IN THE EVENT OF INAPPROPRIATE USE

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the policy may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the policy may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child accidentally accessed inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the following action:

- Inform the Designated Safeguarding Lead immediately.

Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

The issue of a child or young person deliberately misusing online technologies will also be addressed. Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications. The children sign and agree to the points set out in the Children's appropriate use agreement. This agreement is reviewed and signed by the children every term during E-Safety specific session / PSHE sessions.

RESPONDING TO INCIDENTS

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes

Any inappropriate or potentially illegal online activity or suspected abuse which does not relate to a professional can be reported to the Child Exploitation and Online Protection Centre(CEOP) which is part of the National Crime Agency:

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

ACCEPTABLE USE POLICY FOR STAFF AND VOLUNTEERS

The computer system (including laptops and mobile devices) is owned by New Horizons Academy and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's **Acceptable Use Policy** has been drawn up to protect all parties – pupils and staff of the school.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That the schools IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. and
- That staff are protected from potential risk in their use of IT in their everyday work.

New Horizons Academy will try to ensure that staff and volunteers have good access to IT to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

New Horizons Academy reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited. Staff should be aware that files and/or hardware will be handed to the Police or law enforcement agency.

New Horizons Academy reserves the right to amend this Acceptable Use Policy Agreement, at any time. **It is your responsibility to ensure that you are up to date with such changes.**

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use the school systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate young people in my care in the safe use of IT and embed Online safety in my work with pupils.

For my professional and personal safety:

1. I understand that New Horizons Academy will monitor my use of the IT systems, email and other digital communications.

2. I understand that the rules set out in this agreement also apply to the use of school IT systems and equipment when used off-site.

3. I understand that the IT systems are intended for educational use and that I will not use the systems for personal or recreational use.

4. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

5. I will immediately report any illegal, inappropriate or harmful material, website or incident. I become aware of, to the appropriate person.

6. I will be professional in my communications and actions when using the IT systems:
    a. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
    b. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
    c. I understand that email can be forwarded or inadvertently sent to the wrong person, the same levels of language should be applied as for the letters or other media.
    d. I will ensure that when I take and/or publish images of others I do so with their permission and in accordance with the schools policy on the use of digital images/video images. **I will not use my personal equipment to record these images.** Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
    e. I will only use chat and social networking sites in accordance with the school's policies.
    f. I will only communicate with pupils and parents using the official systems. Any such communication will be professional in tone and manner.
    g. I will not engage in any Online activity that may compromise my professional responsibilities.

7. The school has the responsibility to provide safe and secure access to technologies.
    a. I will ensure that 2 Form Authentication is enabled on my school Google Workspace account, and any other school service that requires it, for example CPOMS and Arbor.
    b. I will ensure I have completed all necessary training required including Cyber security and data protection.
    c. When I use my personal devices (incl phone, handheld, laptop, etc), I will follow the rules set out in this agreement, in the same way as if I was using fixed equipment. I

will also follow any additional rules set about such use. I will ensure that any such devices are protected by up to date anti-virus software, are free from viruses and secured via password or PIN code.

d. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

e. I will not try to upload, download or access any materials which are illegal (child sexual abuse, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

f. I will not install or attempt to install programmes of any type on a machine, or store programmes on a PC, I will not try to alter computer settings, unless this is allowed in a specific policy.

g. I will not disable or cause any damage to school equipment, or the equipment belonging to others.

h. I understand that what is on my device is my responsibility and I am accountable.

8. I will only transport, hold, disclose or share personal information about myself or others as outlined in the schools Data Protection Policy. Where personal data is transferred outside the school network, it must be encrypted.

a. I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except where it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

b. I will immediately report any damage or faults involving equipment or software, however this may have happened.

9. When using the internet in my professional capacity:

a. I will ensure that I have permission to use the original work of others in my own work.

b. I will adhere to the licensing terms and conditions of software and services

c. Where work is protected by copyright, I will not download or distribute or save to the school network copies (including music and videos).

d. I will not break copyright by ripping/converting CDs and DVDs and storing them on the school network.

e. I will not attempt to access any streaming services that host or distribute copyright material. e.g. Putlocker style sites.

10. I understand that I am responsible for my actions in and out or work:

a. I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in work, but also applies to my use of school IT systems and equipment out of work and my use of personal equipment in school or in situations related to my employment.

b. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, dismissal. I understand that all illegal activities will be reported to the Police and relevant law enforcement agencies.

11. I will ensure that any use of social media does not:

- bring the school into disrepute.

- breach confidentiality.
- breach copyrights of any kind.
- bully, harass or be discriminatory in any way. and
- cannot be classified as defamatory or derogatory.

Anyone who uses laptops and/or other property from the school will assume all liability and responsibility for safeguarding it while it is loaned out to them.

Please take the following precautions:

- If you leave your laptop in school when not in use, be sure to lock it away securely and do not just leave it out in the classroom or shared spaces.
- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.
- Keep the laptop in your sight when travelling on public transport.
- If you are travelling by car, lock your laptop in the boot when you park.
- Do not use the laptop in locations that might increase the likelihood of damage.
- Keep food and drinks away from the laptop.

If there are any problems with IT related equipment the schools IT dept. must be informed. Repairs **MUST NOT** be undertaken by anyone else.

On termination of employment all IT equipment is to be returned to the IT department directly to be checked and then reissued.

I have read and understand the above and agree to use the school IT systems (both in and out of work) and my own devices (in work when carrying out communications related to work) within these guidelines.

Print Name: _____

Sign: _____

Date: _____