E-safety and ICT Acceptable Use Policy

Latest review undertaken on 15th May 2018

By the Principal & SLT

Next review: Summer term 2018

ocument Status	
Author	J Loisel based on a Model
Date of origin	May 2018
Version	1
Review requirements	Every three years
Date of next review	May 2021
Approval Body	SLT
Publication	Web

Introduction

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as, but not exhaustively, laptops, mobile phones and other mobile devices).

At Hadrian Academy we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The school holds personal data on children, staff and other people to help them conduct their day-to-day activities. The loss of sensitive information is a data breach under the Data Protection Act and General Data Protection Regulation (GDPR) which can result in substantial fines, and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Roles and Responsibilities

The Principal and Governors have ultimate responsibility for e-safety and Acceptable Use.

ICT Subject Leaders are responsible for ensuring that the policy is embedded in the curriculum and that resources, including but not exclusively apps and online programmes, are compliant with the scope of the policy. They are responsible for ensuring that eSafety guidance is given to the pupils on a regular and meaningful basis

The School Business Manager is responsible for ensuring that staff and visitors are aware of the policy and is responsible for its application.

All staff are responsible for bringing ICT/e-safety and/or data breaches and/or breaches of this policy to the immediate attention of the School Business Manager.

Related Policies

This policy should be read in conjunction with the following policies:
Safeguarding
Data Protection
Health and Safety
Home–school agreement
Behaviour (including anti-bullying)

Monitoring

Authorised Hadrian Academy ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

Hadrian Academy ICT authorised staff may, at the direction of the Principal, monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet use and any other electronic communications (data, voice or image) involving its employees, contractors or pupils, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Hadrian Academy ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation 2018, Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Hadrian Academy ICT staff.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach on the part of employees is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the School Business Manager.

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a

memory stick must be checked for any viruses using school provided anti-virus software before being used.

Staff must not interfere with any anti-virus software installed on school ICT equipment.

If staff suspect there may be a virus on any school ICT equipment, they must stop using the equipment and contact the ICT Manager immediately. The ICT Manager provider will advise staff what actions to take and be responsible for advising others that need to know.

Data Security (see also Data Protection Policy)

The school gives relevant staff access to its Management Information System, with a unique username and password.

It is the responsibility of staff to keep passwords secure. Passwords must not be shared with others including other staff at the school.

Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data. Staff have a responsibility for data security under data protection legislation and the GDPR.

Data and personal information relating to pupils or staff at the school should not be shared with external bodies by email. Any such data must be transmitted using the secure ANYCOMMS or Egress system.

Should an agency be unable to access ANYCOMMS or Egress then the approval of the Principal or School Business Manager should be sought to allow data to be shared using an encrypted device.

Portable storage devices must be encrypted.

Staff must not remove personal data relating to pupils, families or other staff from the school premises. The school provides remote access to the school server to facilitate secure home working.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media, in unattended vehicles. Where this is not possible, it must be locked out of sight. Such equipment must not be left in a vehicle overnight under any circumstances.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Any data breaches must be notified to the School Business Manager immediately as they may need to be notified to the ICO. There are strict timeframes for reporting breaches.

Disposal of Redundant ICT Equipment

All redundant ICT equipment must be disposed of through an authorised agency. A certificate of destruction must be obtained to prove secure disposal.

The school maintains an inventory of all its ICT equipment including a record of disposal.

e-Mail

However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

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

Email accounts are password protected and it is the responsibility of each account holder to keep the password secure.

For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.

The school email account must be the account that is used for all school business.

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

School e-mail is not to be used for personal business.

E-mails created or received as part of school roles will be subject to disclosure in response to a request for a Subject Access Request (SAR) or information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail account as follows:

- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

eMail general use: principles and requirements

Staff should check their e-mail regularly.

Staff should use ‘out-of-office’ notifications when away for extended periods.

Staff should never open attachments from an untrusted source; Consult the ICT Manager first.

Staff should not use the e-mail systems to store attachments. They should be detached and saved to the appropriate shared drive/folder.

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

When replying to messages from parents or other official enquiries it is preferred that staff send replies via the school office email.

In other cases staff should send emails from their own school e-mail (never the account of another member of staff) account so that they are clearly identified as the originator of a message.

Staff must keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and ensure that they are appropriate.

Staff must not send or forward attachments unnecessarily. Whenever possible, the location path to the shared drive should be sent rather than sending attachments.

Staff must inform the School Business Manager if they receive an offensive e-mail.

Managing the Internet for pupil use

The school provides pupils with supervised access to Internet resources through the school's fixed and mobile internet connectivity.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Internet: staff use

Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

Staff must not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online

application.

Use of school equipment must comply with the principles and ethos of the school and comply with the requirements of all school policies. This includes (but not exclusively) that on-line gambling or gaming and/or the viewing of any images of an inappropriate or sexual nature is not allowed using school equipment, on or off the premises.

Infrastucture

- The school employs web-filtering.
- The school does not allow pupils or non-ICT staff access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of the SLT or teacher as appropriate.
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the ICT Manager's to install or maintain virus protection on personal systems.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Manager, ICT Subject Leader or School Business Manager.

Social Networking sites and Other Web 2 Technologies

Pupils

- The school endeavors to deny access to social networking and online games websites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils and staff are advised to set and maintain their online profiles to maximum

privacy and deny access to unknown individuals.

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

- Our pupils are asked to report any incidents of Cyberbullying to the school.

Staff

- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Principal.

- Staff may not associate with pupils on any social or similar networks.

- Staff may not post any inappropriate content relating to the School on any site.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).

- Parents/carers are expected to sign a Home School agreement containing the following statement or similar

  → We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community.

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

  - Information and celebration evenings
  - Practical training sessions e.g. How to adjust the Facebook privacy settings
  - Posters
  - School website
  - Newsletter items

Passwords and Password Security

Passwords

- Passwords must contain a minimum of five characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within one month.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep any passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use. Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media
- Ensure removable media is purchased with encryption

- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Principal
- Pupils and staff must have permission from the Principal before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- recorded/ transmitted on a video or webcam
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This Home/School Agreement form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Principal
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- The Class Teacher has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. We do not use publicly accessible webcams in schoolams in school are only ever used for specific learning purposes, e.g. monitoring hens' eggs and never using images of children or adults

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment to the ICT Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in

the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during non-contact and rest periods only.

- During the lesson/contact time personal devices should be switched off and put away beyond use.

- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Under no circumstances does the school allow a member of staff to photograph or video children on their personal device.

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Social Media, including Facebook and Twitter

- Staff **are not** permitted to access their personal social media accounts using school equipment at any time without the express permission of the Principal.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

Telephone Services

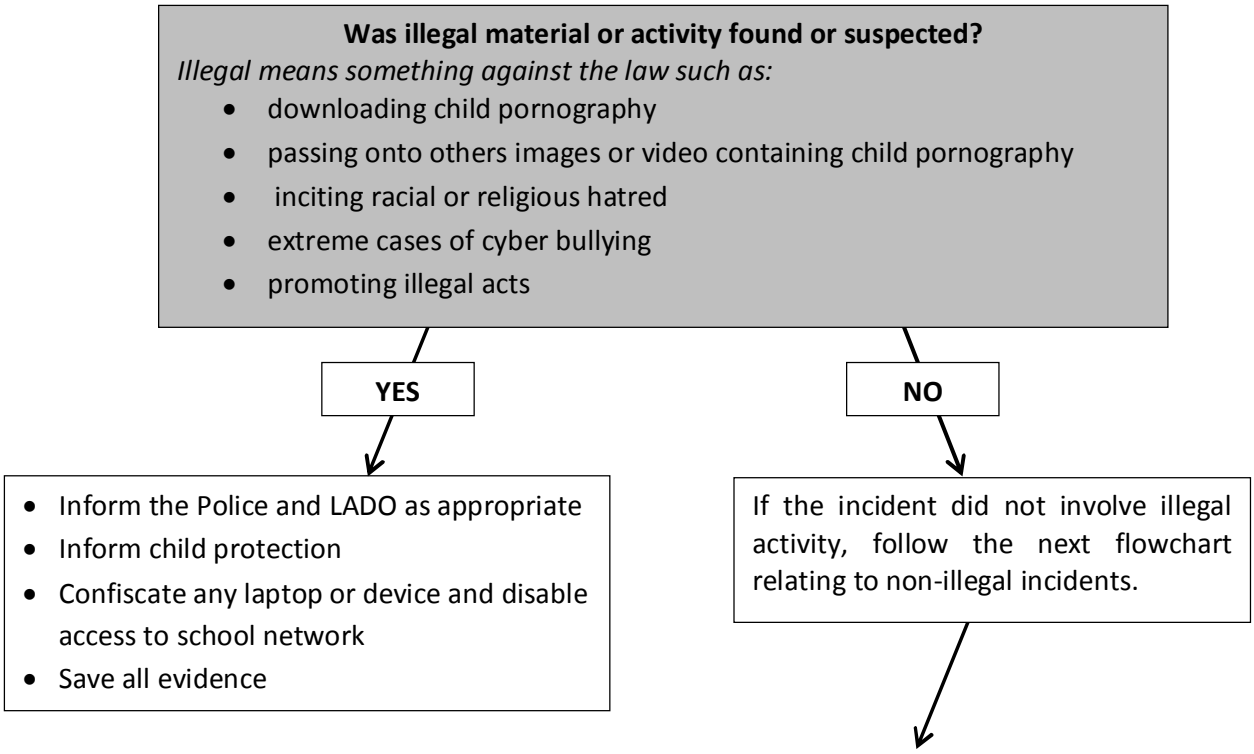
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

Appendix 1: Flow chart for eSafety incident

Managing an eSafety incident

Following an incident the School Business Manager and Principal will need to decide if the incident involved any illegal activity



Managing an eSafety incident that does NOT involve illegal activity.

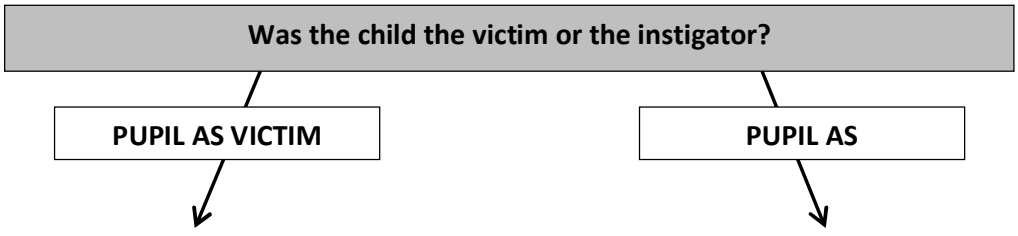
The incident could be:

- Using another person's name or password
- Accessing websites that are against school policy
- Using a mobile phone to take a video
- Using technology to upset or bully

This list is not exhaustive.

The School Business Manager and Principal should:

- Record in the school eSafety Logbook
- Keep any evidence



In school action to support pupil by involving one or more of the following:

- eSafety Coordinator
- Teacher
- SLT
- Child Protection Officer

t wo

- Review incident and identify if other pupils are involved
- Decide on appropriate sanctions or support based on school guidelines
- Inform parents/carers if serious or persistent
- Involve CPO

Acceptable Use Agreement: Staff, Governors and Visitors

Hadrian Academy Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School Business Manager.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I understand that personal data can only be taken out of school when authorised by the Principal or Governing Board and that any personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the School Business Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal or member of the Senior Leadership team. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's ICT and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …… Date ……

Full Name ……..……..(printed)

Job title ……

Summary for visitors

- At this school we have an Acceptable Use policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors.
- Protected and Restricted material must be encrypted if the material is to be removed from the school.
- At this school we use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using ANYCOMMS.

- At this school we store sensitive or personal material in lockable storage cabinets in a lockable storage area.
- At this school all servers are in lockable locations and managed by DBS-checked staff.
- At this school we regularly back-up our data.

- At this school we use approved disposal firms for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is destroyed by a confidential waste service.

- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.