# North Herts Education Support Centre

# Data Security Policy

## INTRODUCTION

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. Everybody in the school community 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.

Both this policy and the Acceptable Use Agreements for staff and pupils are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

## GENERAL

Responsibility for activities undertaken on ICT equipment and access and account rights lies with the individual employee.

Materials considered to be illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Centre or may bring the Centre into disrepute must not be accessed, loaded, stored, posted or sent.

This includes but is not limited to:

- Jokes or chain letters
- Clips or images that are not part of NHESC activities
- Sexual comments or images
- Nudity
- Racial slurs
- Gender specific comments
- Anything that would offend anyone on the basis of their
    - Age
    - Sexual orientation
    - Religious beliefs
    - Political beliefs
    - National origin
    - Disability

## SECURITY

### Security

Staff has a responsibility to keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

Once a member of staff has terminated their employment with the Centre their passwords and logins for all Centre technologies will be changed by the network administrator in order to recover any vital data before being permanently disabled in order to prevent 'zombie accounts' forming.

### Passwords

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 their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Always use your own personal passwords to access computer based services. Never allow somebody else to use your authorised logon.
- Ensure that personal passwords are used each time the system is used. Do not include passwords in any automated logon procedures.
- Change temporary passwords at the first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords on unsecured paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- If you become aware of a breach of security with your password inform the eSafety Coordinator immediately.

All NHESC related passwords should be as strong as possible: a minimum of six characters including at least one capital letter and at least one numerical/symbol character.

## Network Access

Access to the NHESC network is limited to authorised users only. Any user that is granted access will be provided with a logon and password by the Centre. Without accessing the Centre's network a person cannot access the computer systems or Centre internet. Staff logons automatically have access to a wide variety of stored data and information, including the MIS software, and therefore must be protected from unauthorised access.

- Only ICT equipment and software that has been provided and authorised by North Herts Education Centre should be used on site: equipment not owned by North Herts Education Support Centre (such as privately owned ICT, including CD's, PDA's, printers and USB drives) must not be used for Centre work and should never be connected to the Centre computer network. This does not apply to the use of the Centre's wifi via smartphones whilst on site, although any data accessed via personal devices is still subject to the Centre's policies and rules.

- All Centre ICT equipment should be kept physically secure by employees.
- Unauthorised persons are not allowed to use Centre ICT equipment.
- Unauthorised access or unauthorised modifications to the network are not permitted. Breaches of this rule constitute an offence under the Computer Misuse Act 1990.
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- 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

**Protective Marking**

Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents. Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business, however applying too low a protective marking may lead to damaging consequences and compromise of the asset.

The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

The NHESC uses 5 levels of classification:

1. **Open -** The document contains no sensitive or personal information and will be a public document that can be accessed by all staff and students.
2. **Personal -** The document is not protected and does not contain sensitive information; however it is someone’s personal work and so may come with intellectual rights/implied consent attached.
3. **Sensitive -** The document contains information that is identifying and not for public eyes but can be shared amongst Centre staff and trusted external professionals.
4. **Restricted -** The document contains information that is identifying and potentially harmful should it reach public knowledge. Access will be limited to specific roles that require the information for certain tasks.
5. **Confidential** - Any documents containing ultra-sensitive information such as legal documents, medical reports, financial information, or data relating to performance/pay. Access will be extremely limited and may not include all of the Senior Leadership Team.

**Restricted Access**

When accessing any document marked as ‘Sensitive’, ‘Restricted’ or ‘Confidential’:

- 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 sensitive, confidential and classified information you disclose or share with others
- Ensure that sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any sensitive, confidential and classified information contained in documents you fax, copy, scan or print.
- Only download personal data from systems if expressly authorised to do so by the Head or eSafety Coordinator
- You must not post on the internet 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 sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

**Hard Copies**

Any printed or received non-electronic forms of data should still be treated with the same security as an electronic copy would be. This includes restricting access of the document to those not authorised to know the information and ensure the proper storage and (when appropriate) destruction of the document.

**Servers**

- Always keep servers in a locked and secure environment
- Limit access rights on a need basis
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back-up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back-up tapes/discs must be securely stored in a fireproof container
- Back-up media stored off-site must be secure
- Remote back-ups should be automatically securely encrypted.
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data.

**Remote Access**

- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- 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

## COMMUNICATION

### E-mail

The Centre 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.

However you access your 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 Centre email account should 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.
- 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.
- Use your own Centre e-mail account so that you are clearly identified as the originator of a message
- The Centre requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- Staff sending e-mails to external organisations, parents or pupils are advised to (b)cc. one of the Senior Leadership Team.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Open only those attachments that you are expecting and ensure that they are from known sources
- Staff must inform the eSafety Coordinator if they receive an offensive e-mail
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- Activate your 'out-of-office' notification when away for extended periods
- Centre e-mail is not to be used for personal advertising
- Users may not subscribe to mailing lists that are not related to Centre business or activities.
- Mail servers or other systems must not be used to facilitate the widespread distribution of unsolicited or unwanted emails.
- The automatic forwarding and deletion of e-mails is not allowed

Where concluding that e-mail must be used to transmit sensitive or confidential data (only permitted if the user has the authority to do so) users must:

- Exercise caution when sending the e-mail
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail

E-mails created or received as part of your role at North Herts Education Centre will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Delete all e-mails of short-term value
- Do not retain any personal emails
- The sending, receiving and reading of personal emails are only permitted during breaks and outside working hours.
- The number and relevance of emails recipients, particularly those being copied, must be kept to the minimum necessary and be appropriate
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

**Centre Landline Telephones**

When making calls to HCC offices, please use COMNET as this ensures that the call does not go across the public telephone network.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- You may make or receive personal telephone calls provided:
    - They are infrequent, kept as brief as possible and do not cause annoyance to others
    - They are not for profit or to premium rate services
    - They conform to this and other relevant HCC and school policies.
- 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
- Ensure that your incoming telephone calls can be handled at all times
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat.

**Centre Provided Mobile Phones**

- The laws of slander also 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.
- The sending of inappropriate text messages between any member of the school community is not allowed
- All mobile phones must be switched to 'silent' or 'meeting' status during working hours.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Users will need to sign a Centre Provided Technology Agreement before being permitted to take possession of a Centre work mobile

**Answerphones**

- All answer phone greetings must be kept up to date.
- Landline answer phone greetings must include the name of the organisation, the site, the reason there is no-one in the office and that we will get back to them as soon as possible.
- Mobile answer phone greetings must include the person's name, the job title and an alternative number to contact if the call is an emergency.
- When the greeting is recorded, ensure that it is clear, concise and professional.
- All messages must be actively managed on a daily basis – acting as necessary and deleting old messages once the appropriate action has been taken.

**Personal Mobile Phones**

- The laws of slander also 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.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Personal calls are permitted provided they are not frequent, are kept as brief as possible and do not cause annoyance to others.
- Any personal calls should always be taken in the confines of a private area in the building so as not to be overheard by others.
- Mobile phones must not be taken into meetings unless an urgent call is expected. If a call subsequently comes through during the meeting, the member of staff must remove themselves from the room and take the call in private.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

## DEVICES

### PCs/Laptops/Tablets

- NHESC ICT may be used for recreational use during breaks and outside working hours only providing it is not disruptive to others.
- NHESC ICT must not be used to run or participate in any activities that are for personal financial gain.
- Data should be saved frequently onto the network drive to prevent loss of data.
- Data must not be stored on the local drives of PC's; it must always be saved to an appropriate location on the network.
- Users will need to sign a Centre Provided Technology Agreement before being permitted to take possession of a Centre device
- When using portable or mobile ICT equipment within the Centre building, employees must follow the correct signing in and out procedures at all times to ensure that the Centre offices are aware of which personnel are using which piece of equipment.

### Computer Viruses

- Never interfere with any anti-virus software installed on the network.
- Viruses must not be introduced or propagated onto the network.
- All files downloaded from the internet, received via email or on removable media (USB drive, CD or tape) must be checked for any viruses using the anti-virus software provided.
- If there is any suspicion that there is a virus on the network, stop using the equipment and inform the eSafety Coordinator.

### Media

Where necessary permissions must be obtained from the owners or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

### Images

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) the Centre permits the appropriate taking of images by staff and pupils with school equipment. The original copies of the permissions are kept securely in the pupil file and a list of permissions is maintained through the SIMS database which can be produced at any point under the direction of the Head teacher
- 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

- 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 Head images can be taken provided they are transferred immediately and solely to the Centre'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 Head.
- Pupils and staff must have permission from the Head before any image can be uploaded anywhere other than the Centre's network
- Images/films of pupils are stored on the Centre's network in the 'Briar Media' drive
- 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
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks)

**Disposal of Redundant ICT Equipment**

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

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

**Removable Storage**

Members of staff who request it will be issued with a removable data storage device (USB drive) for which they must sign a Centre Provided Technology Agreement.

- Where removable media are used for the transfer of data between ICT equipment, any files containing sensitive, personal or confidential data must be encrypted. This includes USB drives, CDs, tapes or independent disk drives. This includes all data as defined under the Data Protection Act 1998.
- Any data deemed to be confidential, sensitive or financial must not be transferred from the network onto any removable media (such as USB drives or CDs) and used for whatever reason, including home working.
- Any data transferred from the network onto removable media must never be downloaded and stored on employee's private computer equipment for whatever reason.
- If home working is undertaken by employees, they must ensure that all data is copied from any removable media onto the network as soon as possible to ensure that it is completely backed up.
- Any removable media that has been used for backup purposes must be stored safely and securely offsite in accordance with the Centre Critical Incident Plan.

## INTERNET

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the HICS network (Hertfordshire Internet Connectivity Service is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

### Access

The internet must not be accessed using a third party provider via a modem or mobile phone. The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

### Usage

It is at the Head's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- 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
- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Personal data as defined under the Data Protection Act 1998 may only be posted on the internet with the consent of the owner of the data.
- Confidential, classified or sensitive information, including sensitive personal data as defined under the Data Protection Act 1998 and information that is deemed to be financially sensitive must not be posted or disseminated in any way that might compromise its intended audience.
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed
- Visiting any chat room during working hours is only permitted if there is a justifiable business reason for doing so. Visiting sites for your own recreational purposes is not permitted during working hours.
- Making personal purchases of goods on-line is permitted as long as this is done outside working hours.

### Social Media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law
- 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 Head
- Staff at NHESC should not have students as "friends" or "followers" on any social networking site such as Facebook, Instagram, or Twitter.
- Staff should not allow students to contact them via internet communication such as Skype, WhatsApp, Blackberry Messenger or LinkedIn
- Staff should not make comments on social networking sites regarding North Herts ESC or the Centre's staff, students, or stakeholders.

### Website

The Centre website is hosted by an external organisation and maintained by the Data Officer in coordination with the eSafety Coordinator; only these two staff members have the authority to upload anything to the Centre website, and all new information/images/articles must be approved by the Head prior to publishing.

### 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's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the eSafety Coordinator.

## MONITORING

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, 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.

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 Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using Centre ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

## 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.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings. The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

| | |
|---|---|
| Reviewed by: | Ian Gamble |
| Date: | Autumn 2016 |
| Ratified by: | Health & Safety and Premises Advisory Committee |
| Signed: | Iain Sillars 10.11.16 |
| Next Review: | Autumn 2017 |