Horizons Specialist Academy Trust
Providing infinite opportunities

Horizons Specialist Academy Trust

Information Security Policy

Adopted by Finance and General Purposes Committee: 22 May 2018
Date of Next Review: May 2020
Responsible Officer: ICT Manager

Information Security Policy

1. Introduction

1.1 This policy provides a Policy Statement on Information Security and an accompanying set of guidelines for all Trust staff. It is part of a suite of policies and should be read in conjunction with the Data Protection Policy and the Acceptable Use Policy.

2. Policy Statement

2.1 The Horizons Specialist Academy Trust is committed to the protection of information and administrative resources, including paper and electronic resources and the media in which they are stored or transmitted.

2.2 The Trust will hold the minimum personal information necessary to enable it to perform its function and information will be erased in accordance with the data retention policy.

2.3 The Trust will make every effort to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

2.4 The Trust will ensure all personal data is obtained fairly in accordance with the "Privacy Notice" and lawfully processed – See GDPR Data Protection Policy.

2.5 To ensure confidentiality, information will be protected against unauthorised access and only authorised personnel will modify it.

2.6 Staff will receive training and guidance to enable them to understand, and appropriately apply, security measures for the protection of all information.

2.7 Regulatory and legislative requirements as included within the General Data Protection Regulations, the Freedom of Information Act 2000, and the Education (Pupil Information) (England) Regulations 2005 will be met. This may include sharing personal data where it is fair and lawful to do so.

2.8 The Board of Directors is the overall Information Risk Owner and has responsibility for the implementation of this policy and the management of information security across the Trust. The Trust Data Protection Officer has overall responsibility for maintaining this policy and accompanying guidance and providing advice and guidance on implementation.

2.9 Staff are responsible for implementing the policy in their areas of responsibility.

2.10 It is the responsibility of every employee to adhere to this policy.

2.11 This policy and the accompanying guidance will be reviewed, and if necessary updated, every three years.

3 Security and care of equipment

3.1 All items of equipment are the property of the Trust and as such must be kept well-maintained and secure at all times.

3.2 If a member of staff wishes to borrow a piece of equipment, (a laptop, for example) full details will be recorded by the ICT Team.

3.4 If the equipment is lost or stolen then the ICT Manager and Data Protection Officer must be notified. If the equipment was being used for processing personal data then the procedures given below (Security of data) should have been followed to ensure the data was kept safe from disclosure.

3.5 All equipment should be proprietorially marked using an approved security marker to aid identification if recovered, following theft or loss. An asset register which lists all equipment should be kept by the ICT Department – this should include a list of identifying information such as equipment IDs.

4 Security of data

4.1 The Trust has a statutory duty under The General Data Protection Regulations (2016) to ensure appropriate technical and organisational measures are taken to protect personal data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.2 All staff should ensure that any electronic or paper documents which contain personal data or, are otherwise confidential, are protected against unauthorised access. This includes ensuring that paper records are securely locked away, not just at the end of the day but when staff are out of the office, and that when staff are away from a computer it is switched off, or locked against access and password protected.

4.3 Where computers hold personal or confidential data they should be password protected. Staff should not use their own personal memory sticks or removable devices for work purposes and **MUST NOT** use private equipment to store personal data.

4.4 The primary copy of school information should never be stored at home, so school records should be updated as soon as possible with copies of any work that staff do at home, and the home copy deleted.

4.5 Staff must also take reasonable security measures to protect the information they take home from unauthorised loss, access or amendment. Whenever possible, staff should ensure that copies of school information are not stored on their private PC, including in temporary directories.

4.6 When taking paperwork home, staff should ensure that it is stored securely when not in use and is not vulnerable to theft, or accidental access by family members.

4.7 Information in transit should be protected by being locked in a briefcase or car boot. Staff should avoid transferring information or equipment from a car interior to a car boot in a car park where the car will subsequently be left, or leaving information or equipment in a car or car boot at any time when the car is unattended.

4.8 Servers and back-up systems should be kept securely in locked cabinets or a locked area to which only staff have access. Similarly hardware such as laptops which are kept at the school should be locked away at the end of the day, not left on desks or visible through windows.

4.9 Use of emails, scanners or fax systems to transfer data should be limited according to the sensitivity of the data being transferred. Staff must always check that information is being sent to the appropriate recipient. It is strongly suggested that to send sensitive personal data staff use recorded delivery mail which can be tracked or delivered by hand if encryption facilities are not available.

4.10 Staff should not share or give out passwords and should not permit anyone without clearance to access secure information.

4.11 The Computer Misuse Act makes it an offence to access any computer system for which access authorisation has not been given. Thus any attempt to interfere with or try to bypass the security controls on a computing system is an offence. Similarly trying to obtain information, such as users' passwords or accessing or modifying files belonging to other people who have not given access authorisation is also an offence.

5. Secure Disposal

5.1 All confidential waste paper should be shredded and / or disposed of through a confidential waste service. This includes personal data due for destruction, duplicates of personal data and other confidential information.

5.2 Computer systems must be fully cleansed of any information before they are disposed of or re-sold. Approval and support for this must be obtained from the ICT Manager. Discs, memory sticks and other removable devices should be destroyed if they are intended for disposal.

6. Security of buildings

6.1 All staff must wear ID badges. Staff should be prepared to challenge any member of the public within the school to ensure that they have a right to be there.

6.2 Any contractor should carry identification and show this on request. All contractors will need to sign in and sign out at the office.

6.3 Staff should ensure that windows and external doors are locked when a classroom or office is empty, and at the end of school, and that offices, filing cabinets and cupboards are also kept locked if required.

6.4 Any security concerns including break-ins and loss of computer equipment must be reported to the Principal.

7. Email Security

7.1 Staff must bear in mind that email is a formal record of correspondence and can be subject to request under Data Protection and Freedom of Information legislation – emails are also retained as records on staff, pupil and school files.

7.2 Staff must not send anything which would be unlawful or discriminatory, or whose content is defamatory or libellous. Work emails should not be used for forwarding chain letters or similar 'spam'. The Telecommunications Act 1994 makes it an offence to transmit messages or other matter via a public telecommunications system that is indecent, obscene or menacing. This includes causing annoyance, inconvenience or needless anxiety to another by a message that the sender knows to be false

7.3 If members of staff receive an email which breaches the Trust's policies or breaks the law they are advised to speak to a senior staff member of staff or the ICT Manager before responding. This includes 'spam' emails, particularly those purporting to be from banks, or any email asking the recipient for money.

7.4 Staff should re-read any message before sending, checking for clarity and content (including grammar), and ensure that the message is being sent to the appropriate recipient.

7.5 Do not use email if the information being sent is personal or confidential, unless you are certain the information will be secure for example through password protection.

7.6 Do not use email where there may be a contractual or legal need to provide a written and signed document or prove the identity of the sender.

8 Internet security

8.1 Access to the Internet must be used responsibly and legally. Staff must not take *any* action which could bring the Trust into disrepute, cause offence, interfere with the organisation's work or jeopardize the security of data, networks, equipment or software.

8.2 Under no circumstance should staff make use of the school internet to access chat lines or similar services.

8.3 With the advent of e-commerce, staff should beware of committing the school to purchase or acquire goods or services without proper authorisation. Purchase order must be raised for all goods and services.

8.4 Staff must not attempt to download or install unauthorised software from the internet.

8.5 Staff should be aware that, as with paper sources, not all information on the internet is accurate, complete or reliable. Users should ensure its validity, as they would printed publications, before using it.

8.6 At any time and without prior notice, the Trust reserves the right to examine e-mail, personal file directories, and other information stored on the Trust network and equipment. Permission to examine such information will only be granted by the Chief Executive Officer.

9 Security of records

9.1 Access to data, and particularly personal data, should be limited to staff who have a genuine ‘need to know’. Staff should be aware that all computer systems permit audit trails to be checked to see who has altered or updated data.

9.2 Changes to data, and particularly personal data, should be carried out promptly and recorded appropriately so the reason for the change and its originator is known.

9.3 Records should be properly managed to enable staff to find or identify information quickly and accurately. Best practice dictates that student and staff records are kept in one location – multiple locations will lead to duplication or discrepancies between files.

10 Reporting & responding to security breaches

10.1 Any security breaches or loss of personal data must be immediately reported to the CEO who in turn will inform the Trust Data Protection Officer.

10.2 A security breach would be caused when [and this not an exhaustive list]:

- A laptop containing personal data is lost or stolen
- A USB [memory stick] containing personal data is lost or stolen
- A vehicle containing a laptop or paper files is stolen
- A laptop or paper files are stolen from a private property
- An email is sent [either internally or externally] with files attached containing personal data and the email is sent to the wrong email address
- An email is sent [either internally or externally] with files attached that contain personal data which is far in excess of that necessary in order for the business function to be carried out
- An email is sent [either internally or externally] which should be sent “bcc” to a large number of people, is instead, sent “to” and so the recipient is aware who

else has received the email and their personal email address or other personal details

- Personal data is shared outside of the school for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
- Personal data is transferred electronically outside the school and is not encrypted when it should be
- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
- A member of staff uses personal data for a personal rather than a school or Trust business reason

10.3 Any loss of or damage to technical equipment should be notified to the ICT service.

10.4 The Trust Data Protection Officer with support from the HR Manager and where necessary the ICT Manager for cases involving breaches of IT security will investigate the security breach / loss of data through the process detailed. The investigation will determine whether to notify the Information Commissioner. The following guidance will be followed when considering a referral to the Information Commissioner.