Information Security Policy

This policy was adopted by the Trustees of Ivy Education Trust on 20 February 2024

Review date: See Amendment Record

Introduction

Information security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted each day.

This policy explains staff responsibilities that are already in contracts of employment and reflects statutory obligations.

Details of how personal data is used is contained within privacy notices. The data protection policy sets out how the Trust's statutory obligations are managed.

The policy applies to all Trust staff which includes trustees, governors, agency staff, contractors, work experience students and volunteers when handling personal data.

Information security breach

Information security breaches can happen in a number of different ways.

Examples include:

- sending a confidential email to the wrong recipient
- letters sent to the wrong address with health and SEN data included
- overheard conversations about a member of staff's health
- an unencrypted laptop stolen after being left in a car
- hacking of Trust systems
- leaving confidential documents containing personal data in a car that was stolen

These would all need to be reported to the Trust Data Protection Officer (DPO). Anything which a staff member becomes aware of even if they are not directly involved in needs to be reported. For example, if they know that document storage rooms are sometimes left unlocked at weekends.

The sooner the breach is notified to the right person, the sooner and more effectively it can be managed.

In certain situations, it is necessary to report a breach to the Information Commissioner's Office (ICO), the data protection regulator, and notify those whose information has been compromised within strict timescales. This is another reason why it is vital breaches are reported immediately.

Privacy on a day-to-day basis

Staff must be aware of data protection and privacy whenever they handle personal and sensitive data.

Sensitive personal data

Data protection is about looking after information about individuals. Even something as simple as a person's name or their attendance record is personal data. However, some personal data is more sensitive. This is called **sensitive personal data** in this and the data protection policy. Greater care about how that data is used is required.

Sensitive personal data includes:

- safeguarding and child protection matters
- serious or confidential physical or mental health conditions
- special education needs (SEN) information

- details of serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved
- financial information about parents/carers and staff
- racial or ethnic origin
- political opinion
- religious beliefs or beliefs of a similar nature
- trade union membership
- genetic information
- sexual life or orientation
- actual or alleged criminal activity
- biometric information (e.g. fingerprints used for cashless catering)

Minimising the amount of personal data held

Restricting the amount of personal data we hold on an individual is needed to help keep the personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please speak to the DPO.

Basic IT expectations

Lock computer screens: A staff member's computer screen should be locked when it is not in use, even if they are only away from the computer for a short period of time. To lock a computer screen, press the "Windows" key followed by the "L" key.

If staff are not sure how to do this speak to a member of the IT department.

Be familiar with the technology: Staff should make sure that they familiarise themselves with anysoftware or hardware that they use. In particular, they need to understand what the software is supposed to be used for and any risks.

For example:

- electronic registers – set to the correct view so students cannot see personal data of classmates
- virtual classrooms – be careful that confidential information is not uploaded for students to access
- shared drives – ensure you know where to store information containing sensitive personal data

Hardware and software not provided by Ivy Education Trust: Staff must not use, download, or install anysoftware, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to IT systems without permission.

Private cloud storage: Staff must not use private cloud storage or file sharing accounts to store or share Trust documents.

Portable media devices: The use of portable media devices (such as USB drives) is not allowed unless those devices have been given to staff and training received on how to use those devices securely. The IT Department will protect any portable media device given to you with encryption.

IT equipment: If staff are given IT equipment to use (this includes laptops, printers and phones) staff must make sure that this is recorded on IT equipment asset register. IT

equipment must always be returned to the IT Department even if you thinkthat it is broken and will no longer work, and the asset register updated accordingly.

Passwords

Passwords should be long and difficult to guess. Staff should not choose a password which is so complex that it's difficult to remember without writing it down. Passwords should not be disclosed to anyone else.

Staff should not use a password which other people might guess or know, or be able to find out, such as their address or birthday.

Staff must not use a password which is used for another account. For example, staff must not use a password used for their private email address or online services for any school account.

Passwords (and any other security credential staff are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

Emails

When sending emails staff must take care and check to ensure that the recipients are correct.

Sending an email to multiple recipients, staff must be sure to check that they are using the correct 'To:' 'CC:' or 'BCC:' function.

If the email contains any personal data then staff should ask themselves is this the best communication method. Sometimes it is unavoidable so staff should ensure the email is sufficiently encrypted and ask an authorised staff member to check the email addresses have been entered accurately. When sending personal data over email, staff should consider inputting the information into an attachable document which is password protected.

Staff must not use a private email address for any Trust related work. A school/trust email address must only be used. This also applied to governors/trustees.

Paper files

Keep under lock and key: Staff must ensure that papers which contain personal data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

Disposal: Paper records containing personal data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal data should never be placed in the general waste.

Printing: When printing documents, staff must collect everything from the printer straight away, otherwise there is a risk that confidential information being read or picked up by someone else. If you see anything left by the printer which contains personal data then you must securely destroy it.

Put papers away: Staff should always keep a tidy desk and put papers away when they are no longer needed.

Post: Staff also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If staff need to send something in the post

that is confidential, consider asking the IT team to put it in on an encrypted memory stick or arrange for it to be sent by courier.

Working off-site

Staff might need to take personal data off-site for various reasons such as remote working or supervising a school trip. This does not breach data protection law if the appropriate safeguards are in place to protect personal data.

For school trips, the trip supervisor should decide what information needs to be taken and who will be responsible for looking after it. Any personal data taken off-site must be returned back to school.

When a staff member works from home, they should check with the DPO whether any additional arrangements need to be put in place to ensure the security of data.

Only take the minimum: When working away from site staff must only take the minimum amount of information with them. For example, if only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.

Working on the move: Staff must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, the individual should ensure that no one else can see the laptop screen and they should not leave any device unattended where there is a risk of theft.

Paper records: If staff need to take hard copy records with them then they should make sure that they are kept secure.

For example:

- documents should be kept in a locked case
- information should be kept with them at all times
- the individual must keep the documents out of plain sight
- if the individual has a choice between leaving documents in a vehicle and taking them with them (e.g. to a meeting) then they should be taken with them

Public Wi-Fi: Staff must not use public Wi-Fi to connect to the internet. If working in a public café, the individual should use their 4G or 5G.

Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action.

A member of staff who deliberately or recklessly obtains or discloses personal data without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

This policy does not form part of any employee's contract of employment.

We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by email.

AMENDMENT RECORD

Date	Reviewed by	Nature of Change	Next Review
30.01.2024	PHP Law/DPO/FAR Committee	New policy to replace previous version.	As required and no later than January 2026.