



YORKSHIRE WOLDS TEACHER TRAINING

Data Protection Policy

Version 1.1

<p>Important: This document can only be considered valid when viewed on the VLE. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.</p>	<p>Alison Fletcher (Director of Yorkshire Wolds Teacher Training)</p>
<p>Name and Title of Author:</p>	<p>YWTT Executive Board</p>
<p>Name of Responsible Committee/Individual:</p>	<p>September 2018</p>
<p>Implementation Date:</p>	<p>July 2019</p>
<p>Review Date:</p>	<p>All stakeholders</p>
<p>Target Audience:</p>	<p>ICT Acceptable Use Policy Freedom of Information Act 2000 Publication Scheme FOI Policy</p>
<p>Related Documents:</p>	<p>www.ico.org.uk</p>
<p>References:</p>	

Contents

1. POLICY STATEMENT	3
2. PURPOSE AND SCOPE	3
3. AIMS & OBJECTIVES OF THE POLICY	3
4. LEGISLATION AND GUIDANCE	3
5. DATA PROTECTION PRINCIPLES	4
6. THE DATA CONTROLLER	4
7. ROLES AND RESPONSIBILITIES	4
8. DEFINITIONS	6
9. COLLECTING PERSONAL DATA	7
10. SHARING PERSONAL DATA	8
11. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS ...	8
12. PARENTAL REQUESTS TO SEE THE EDUCATION RECORD	Error!
Bookmark not defined.	
13. BIOMETRIC RECOGNITION SYSTEMS	10
14. CCTV	10
15. PHOTOGRAPHS AND VIDEOS	11
16. DATA PROTECTION BY DESIGN AND DEFAULT	11
17. DATA SECURITY AND STORAGE OF RECORDS	12
18. DISPOSAL OF RECORDS	13
19. PERSONAL DATA BREACHES	14
20. TRAINING	14
21. MONITORING ARRANGEMENTS	14
Appendix 1: Personal data breach procedure	15
Appendix 2: Clear Desk Procedure	18

1. POLICY STATEMENT

Our vision is to *inspire* each other and our students so each of us *aspires* to reach a potential which is not limited but is given wings by creativity and a shared sense of purpose.

Our core purpose is to prepare trainees to become highly effective teachers with a love of learning who will continue to develop their skills throughout their career, through exposure to excellent practice, observation, mentoring, coaching, practice, reflection and sharing with peers. Our trainees will be enthusiastic and passionate practitioners and will find innovative and creative ways to communicate with learners and enable them to make excellent progress. We will seek to equip our trainees with a wide range of teaching and learning strategies as well as the inter-personal skills required to motivate and inspire students.

Yorkshire Wolds Teacher Training is committed to developing its trainees into excellent teachers through a creative, effective and rigorous programme underpinned by supportive and highly experienced teacher educators. Our aim is to create models of outstanding practice across the partnership and to meet the needs of our partner institutions as well as training the school leaders of the future.

2. PURPOSE AND SCOPE

Yorkshire Wolds Teacher Training (YWTT) understands its obligations under the current Data Protection Act 1998 (the Act) and the provisions of the Data Protection Bill 2017-19. The Act regulates the use of personal data and this policy aims to inform anyone who comes into contact with data within YWTT of their responsibilities, ensuring that they adhere to the Act, minimising the risk of unintentional breaches.

YWTT has individuals in various roles that come into contact with and use confidential personal information about trainees and candidates who have applied to YWTT on a regular basis. YWTT also holds information about trainees and trainees are required to inform YWTT of any relevant changes to ensure information retained is accurate (e.g. address, contact details, bank details).

3. AIMS & OBJECTIVES OF THE POLICY

YWTT aims to ensure that all personal data collected about trainees is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Bill 2017-19.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

4. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the provisions of the Data Protection Bill 2017-19. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

5. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that YWTT must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how YWTT aims to comply with these principles.

6. THE DATA CONTROLLER

The Education Alliance is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. YWTT is part of the Education Alliance.

7. ROLES AND RESPONSIBILITIES

This policy applies to YWTT Executive Board Members, and **all staff** employed by YWTT, and to external organisations or individuals working on our behalf. Anyone who uses YWTT data who do not comply with this policy may face disciplinary action.

- 7.1** The **YWTT Executive Board** will ensure that appropriate policies, procedures, systems and processes are in place within YWTT to minimise the risk of a breach of the Act and the GDPR.
- 7.2** The **Director of YWTT** is responsible for ensuring that staff are aware of the expectations surrounding data protection and the potential consequences should a breach occur.

7.3 The **Director of YWTT** has overall responsibility for ensuring that YWTT complies with all relevant data protection obligations. They are the representative of the data controller on a day-to-day basis.

7.4 The **Director of YWTT** is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. This will also include the circulating appropriate policies, documentation and information to staff in relation to the Act.

The Director of YWTT will log and report all data breaches to the YWTT Executive board

The Trust's Data Protection Officer is **Alex Dick** and is contactable via: on 01482 374211 or email DPO@theeducationalliance.org.uk

7.5 The **South Hunsley IT Department** is responsible for ensuring that electronic data systems adhere to the requirements of the Act and that there are appropriate mechanisms in place for monitoring and access, such as audit trails, access rights, password and security measures and IT related policies and procedures.

7.6 **All Trainees and staff working on behalf of YWTT** are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing YWTT of any changes to their personal data, such as a change of address
- Compliance with YWTT privacy notice for trainees
- Contacting the YWTT DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - With any questions about the operation of this policy,
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

- Ensuring contracts / agreements are in place with third parties where personal data is being shared

8. DEFINITIONS

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</p>

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

9. COLLECTING PERSONAL DATA

9.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that YWTT can **fulfil a contract** with the individual, or the individual has asked The Education Alliance to take specific steps before entering into a contract
- The data needs to be processed so that YWTT can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that YWTT, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of YWTT or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student/student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

9.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule and any relevant laws or regulations

10. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a trainee that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our trainees or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

11. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the trust or school holds about them. This includes:

- Confirmation that their personal data is being processed

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the Director of YWTT. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If YWTT staff receive a subject access request they must immediately forward it to the Trust's Governance team for logging.

11.2 Responding to subject access requests

When responding to requests, we:

- Respond without delay and within 1 month of receipt of the request
- Under normal circumstances will provide the information free of charge
- Tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

The YWTT Executive board will make the decision if the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

The YWTT Executive board will deem a request to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When a request is refused, the YWTT team will write to the individual to tell them why, advising them they have the right to complain to the ICO, with details to enable them do this.

11.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 9), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. BIOMETRIC RECOGNITION SYSTEMS (currently needed for them to use our resources in the Hunsley library – may could remove when we move)

Where trainees use the South Hunsley school's biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice and The Education Alliance CCTV policy for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and signage is prominent as you enter any of our sites that CCTV is in use.

Any enquiries about the CCTV systems in any school should be directed to the IT manager of the relevant school.

14. PHOTOGRAPHS AND VIDEOS

As part of YWTT activities, we may take photographs and record images of individuals within our training base.

We will obtain written consent from trainees for photographs and videos to be taken of trainees for communication, marketing and promotional materials.

Uses may include:

- Within YWTT on notice boards and in YWTT brochures, newsletters, etc.
- Outside of YWTT by external agencies such as newspapers and campaigns
- Online on our YWTT website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information.

15. DATA PROTECTION BY DESIGN AND DEFAULT

We have put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 8)
- Completing privacy impact assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

16. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are in a secure environment
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access, all staff will adopt the Clear Desk Procedure (Appendix 2)
- Where personal information needs to be taken off site, it must be kept secure at all times
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our IT policy/acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 10)

17. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Destruction of confidential waste must be complete:

- Paper must be incinerated or shredded
- Destruction of electronic records, storage devices and tape must be by incineration or the use of a specialise equipment or software that will destroy the information
- CD's can be cut up and disposed as per paper waste
- It is not necessary to incarnate crosscut shredded paper – shredding is an acceptable method of total destruction of confidential information and the remains are safe to be sent for recycling

Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction:

- Confidential waste should be kept separate from other waste material and confidential waste bins used where possible, otherwise waste should be bagged and clearly labelled “confidential waste”
- Bagged waste awaiting collection must be kept secure at all times
- Only authorised YWTT authorised personnel or an approved contractor should handle the waste

If destruction is to take place off site, the waste must be escorted and its destruction witnessed by an authorised member of staff unless the contractor is specialised in the secure destruction of confidential waste and will provide destruction certificates.

If the destruction is to take place onsite, the contacted supplier must be specialised in the secure destruction of confidential waste and their procedures must confirm to recognised industrial standards.

If a non-specialised waste disposal service is used, the following standards apply:

- An authorised member of staff must escort the waste offsite and witness its destruction
- A certificate of destruction must be provided
- The confidential waste bags must be kept secure and separate from any other waste whilst waiting to be destroyed
- The bags must not be opened prior to destruction. Hand sporting of the waste for recycling or for any other purpose is unacceptable practice

18. PERSONAL DATA BREACHES

YWTT will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

19. TRAINING

All trainees are provided with data protection training as part of their induction process.

All YWTT staff are provided with data protection training as part of their induction process and they will continue to have on-going mandatory refresher training.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or YWTT's processes make it necessary.

20. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** with recognised trade unions at local secretary level.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
 - The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
 - The DPO will alert the Director of YWTT, CEO and the Executive Committee (and the Chair of the Board of Trustees if deemed necessary by the CEO)
 - The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
 - The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
 - The DPO and CEO will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO and CEO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. The DPO will

document breaches and outcome decisions which will be held on a centrally by the DPO for all the schools within the trust.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on a centrally held record for all the schools within the trust.

- The DPO and the Executive Committee will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Clear Desk Procedure

Confidential and sensitive information, whether held electronically or in paper format, must be secured appropriately when staff are absent from their workplace and at the end of each working day.

In order to ensure that this is applied within the Trust, the below procedure is to be followed:

- Employees are required to ensure that all confidential and sensitive information in hardcopy or electronic form is secure in their work area at the end of the day or, if they leave their desk, at any point during the working day.
- To reduce the risk of a breach of confidentiality and to adhere to the Data Protection Act, confidential and sensitive documents, including person identifiable information, when no longer required, must be securely disposed of immediately.
- Computer desktops must be logged off or have a password locked screensaver when the employee is away from their work area.
- Filing cabinets, office cupboards or desk drawers must be kept closed and locked when not in use or unattended if they contain any confidential and sensitive information.
- Keys for the locked areas must not be left unattended at the employee's work area. If the employee will be on annual leave or working outside the office, if appropriate, the keys should be left with a colleague in the same department or in a lockable key cabinet on site.
- When any confidential and sensitive information is requested over the phone, all employees must ensure they are speaking to the correct person to whom this information can be disclosed. This can be confirmed by calling the recipient back on a number that is already recorded on SIMS or asking relevant questions to which one the recipient would know the answer.
- Documents that contain confidential and sensitive information and which are being sent via email must be encrypted (password protected). Employees must send a second email to give the password once the document has been emailed across. The password must not be sent in the same email as the document.
- Staff are encouraged not to store data locally on their device and if not based at their main place of working, to save data using the remote access.
- When saving confidential and sensitive information to the Trust's Network / SharePoint / Google Drive, it is the responsibility of the employee to check who has access to the file and ensure that the information is only shared with those authorised to access the information.
- No confidential or sensitive information is to be saved to USB drives or other external drives, even if the documents are encrypted (password protected). If there is a requirement for any of this information to be saved to external drives, the employee is required to obtain permission from the Trust's Data Protection Officer before proceeding.
- All employees are advised to assess whether any confidential or sensitive information needs to be printed before doing so. If it is not required to print the

information, the Trust advises that the information is stored electronically. If printed, it must be stored securely and disposed of securely when no longer required.

- Desks and other work spaces must be sufficiently tidy at the end of each working day to permit the Trust's cleaning staff to perform their duties.

Printers and Photocopiers

For Follow Me Printing (secure printing), all Trust employees receive an access card and/or PIN code to enable the printing of documents through password protection. All employees must keep their codes confidential. If these codes are shared with colleagues and a breach of confidentiality occurs, this will be dealt with through the Trust's Staff Disciplinary Policy.

When sending scanned confidential or sensitive information from the printer to an email address, all employees must send the documents from the printer to their work email address and then forward on to the required person to ensure that only the correct recipient receives the information. It is not recommended that documents are scanned and sent from the printer to the recipient directly.

If it is necessary to copy any confidential or sensitive information, the employee must remain at the printer whilst the copy is being completed and ensure all copies are removed from the printing tray on completion.