

Page 1 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Authorised by: CEO, Paul Storey Chair of Trustees, Peter Brown	Version: 1.4	Issue Date: January 2024	Review Date: January 2025
--	---------------------	------------------------------------	-------------------------------------



INFORMATION GOVERNANCE AND DATA PROTECTION POLICY & PROCEDURE

**Charitable Incorporated Organisation
Charity Number: 1159808**

Page 2 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

CONTENTS

Section A

Data Protection Policy and Procedure

- Introduction
- Purpose
- UK GDPR and the Data Protection Act 2018
- Scope
- Roles and Responsibilities
- Personal Data
- Right of access
- Marketing and Consent
- Lawful Basis for Processing
- Data Breaches
- Use of Personal Data
- Registration with the Information Commissioner's Office (ICO)

Section B

Email and Internet Policy

- Introduction
- Email Procedure
- Internet Procedure
- Unauthorised Use
- Monitoring
- Security
- Implementation of policy

Section C

Social Media Policy and Procedure

- Social Media Policy
- Social Media Procedure
- Disciplinary Action

Section D

Use of Mobile Phone policy and procedure

- Use of Mobile Phone policy
- Procedure

Section E

Password Schedule

Review and Update

Page 3 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Regulatory Requirements

References

Appendix 1 Data Protection Do's and Don'ts

Appendix 2 Record Types

Appendix 3 Confidentiality Agreement

Appendix 4 Confidentiality Agreement for third parties

Introduction

R-evolution needs to gather and use certain information about individuals (personal data). This can include customers, employees, prospective employees, contractors, suppliers and any other third party that the organisation has a relationship with or needs to contact. We take our responsibilities to protect personal data and use it lawfully very seriously.

This policy describes how R-evolution manages those responsibilities.

Purpose

During carrying out our business, R-evolution collects, stores, and uses information relating to individuals. The collection and use of this information are regulated by the UK *General Data Protection Regulation (UK GDPR)*, the *Data Protection Act 2018* and by various other data privacy laws and regulations. These laws and regulations impose restrictions and controls on the way we can process personal data. These laws also grant rights to the individuals whose information is processed by our organisation.

This policy aims to serve as a guide with brief details about UK GDPR and its implications for our organisation. It is also intended to provide employees with basic information on the impact of UK GDPR on their daily business, to enable them to use personal data in a way that does not put us in breach of UK GDPR.

To maintain compliance with UK GDPR we must ensure that:

- You must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned.
- You must be clear, open, and honest with people from the start about how you will use their personal data.

Page 4 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

If we fail to comply with the UK GDPR then this could have serious consequences for our reputation and business. In extreme cases the organisation or individual members of staff could be found to have committed a criminal offence.

The ICO also have published some helpful guidance on UK GDPR to make this content more accessible. These links are available in the References below.

UK GDPR and the Data Protection Act 2018

General data protection regime applies to most UK businesses and organisations. This covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

The organisation endorses fully and adheres to the seven principles of data protection as set out in the Article 5 of the UK GDPR:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Scope

The policy applies to all organisation employees, service providers, contractors and third parties that access, use, store, or process personal data on behalf of R-evolution.

The policy covers:

- all personal data created or received by the organisation in any format (including paper), whether used in the organisation, filed in filing cabinets, stored on portable devices and media, transported from the organisation physically or electronically or accessed remotely.
- personal data held on all organisation IT systems; and
- any other IT systems on which personal data is held or processed.

Page 5 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Roles and Responsibilities

CEO

The CEO is responsible for:

- Maintaining and managing the policy.
- Co-ordinating and responding to Data Subject Access Requests, Information Rights Concerns, Information Notices, Assessment Notices or Enforcement Notices.
- Reporting and updating the Board of Trustees in the event of a Data Breach notification.
- Co-operating with authorities during an investigation.
- Notifying the ICO in the event of any Personal Data Breach incident if necessary.
- Identifying and assessing any privacy related risks and reporting to the Organisation Management Team.
- Working with the Management Team to provide data protection awareness.

Organisation Management Team

The Organisation Management Team are responsible for:

- Implementation of this policy on a day-to-day basis within the business areas of the organisation for which they are responsible.
- Ensuring that all employees who report to them are made aware of and are instructed to comply with this policy.
- Providing training to promote ongoing Data Protection Awareness.

Staff

Each member of staff is responsible for:

- Complying with the terms of this policy and all relevant UK GDPR data protection legislation and applicable legislation
- Always valuing and protecting the privacy and confidentiality of the information they process
- Obtain and process personal data only for specified purposes
- To only access personal data that is specifically required to carry out their activity
- Record personal data correctly in both electronic and manual records
- Ensure that personal data is stored securely
- Ensure that personal data is not disclosed to unauthorised third parties

Page 6 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

- Ensure that personal data is always sent securely.

Employees whose roles involve access to personal data must always follow these principles when processing or using employees' personal information.

Failure to observe the guidance in this policy could mean that an individual is criminally liable for deliberate unauthorised disclosure and subject to disciplinary action.

For a summary of guidance to comply with best practice, please refer to our **Appendix 1 Data Protection Do's and Don'ts**

Employees, volunteers, trustees, trainees and third parties will be asked to sign a confidentiality agreement, see appendices 3 and 4.

Personal Data

What is personal data?

- The UK GDPR applies to the processing of personal data that is:
 - wholly or partly by automated means; or
 - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
 - can be identified or who are identifiable, directly from the information in question; or
 - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are more sensitive, and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.

Page 7 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

- However, information about individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The UK GDPR provides a non-exhaustive list of identifiers, including:
 - name
 - identification number
 - location data
 - an online identifier.
- 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.

Can we identify an individual directly from the information we have?

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

Can we identify an individual indirectly from the information we have (together with other available information)?

- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.

Page 8 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

What is the meaning of ‘relates to’?

- Information must ‘relate to’ the identifiable individual to be personal data.
- This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether data relates to an individual, you may need to consider:
 - the content of the data – is it directly about the individual or their activities?
 - the purpose you will process the data for; and
 - the results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.
- Inaccurate information may still be personal data if it relates to an identifiable individual.

Right of access

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- This is commonly referred to as a subject access request or ‘SAR’.
- Individuals can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- In most circumstances, you cannot charge a fee to deal with a request.

Page 9 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

- You should respond without delay and within one month of receipt of the request.
- You may extend the time limit by a further two months if the request is complex or if you receive several requests from the individual.
- You should perform a reasonable search for the requested information.
- You should provide the information in an accessible, concise, and intelligible format.
- The information should be disclosed securely.
- You can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

Data Subject request must be made via our CEO.

Marketing and Consent

Under UK GDPR we must have positive opt-in to provide marketing content to new customers. Where new customers have not 'opted-in' to marketing we cannot assume consent. Current customers can be sent marketing under legitimate interests. Our marketing activities over electronic mail are subject to UK GDPR, data protection and PECR legislation.

Lawful Basis for Processing

As well as consent, we rely on other lawful bases for processing personal data, these are:

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering a contract.

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Data Breaches

It is important that a data breach (even if only suspected) is reported to the CEO. This is necessary so that we attempt to contain the breach and fulfil our legal obligation to notify the ICO (if necessary) within 72 hours in compliance with UK GDPR.

Page 10 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Use of Personal Data

Any unauthorized disclosure will normally be regarded as a disciplinary matter and may be considered gross misconduct in some cases.

All staff must use personal data responsibly and lawfully and not disclose it to unauthorised personnel either inside the organisation or outside the organisation.

Only organisation approved devices may be used to process personal data of customers or staff. The use of personal devices is not permitted to access organisation systems or data. Personal devices can be used with prior approval from a line manager to produce documents at remote locations, examples would be lesson plans, guides, supporting materials etc.

Registration with the Information Commissioner's Office (ICO)

R-evolution would be exempt from Registration with the ICO as being established as a not-for-profit organisation. A not-for-profit organisation can make a profit for its own purposes, which are usually charitable or social, but the profit should not be used to enrich others. Any money that is raised should be used for the organisation's own activities.

However, R-evolution uses CCTV on the organisational premises for the purpose of crime prevention, therefore is registered with the ICO and pays the appropriate fee.

Email and Internet Policy

Introduction

The use of the email system and the internet within this organisation is encouraged, as this use facilitates communication and improves efficiency. Inappropriate use, however, causes problems ranging from lack of productivity to legal claims against the organisation. This policy sets out the organisation's guidelines on the correct use of email and the internet, and the organisation's response to inappropriate use.

Procedure

Email

1. The email system is available for communicating matters directly concerned with the business of this organisation. The style and content of email messages must be consistent with the high standards that this organisation expects from written communications.
2. To reduce email overload and aid productivity, email messages should only be sent to those employees for whom they are relevant. Only send attached files where necessary.
3. Although email encourages rapid communication, the contents of email messages should be written with care as messages sent without proper consideration can cause unnecessary misunderstandings. Email should not be used as a substitute for face-to-face communication.
4. Where necessary, email messages should include a confidentiality statement

Page 11 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

5. Employees should note that offers or contracts transmitted via email are as legally binding on the organisation as those sent on paper.
6. Email contact lists are the property of the organisation even if created by the employee. Employees may not copy or remove any contact list in its entirety for use outside the organisation without the express permission of the CEO.
7. Any failure to follow these guidelines satisfactorily can result in disciplinary action up to and including summary dismissal.

The internet

1. Unless it comes from an official source, information obtained from the internet (generally the World Wide Web) should be cross-checked before being used. Where that is not possible, full details of the source should be recorded.
2. Even when used for work-related purposes, browsing the Web can be highly time consuming and therefore should be undertaken responsibly.

Unauthorised use

1. The organisation will not tolerate the use of the email or internet system for illegal or inappropriate activities. Such activities include (but are not limited to):
 - a. sending or forwarding any message that could constitute bullying or harassment (e.g., on the grounds of sex, race or nationality, religion, sexual orientation, age, or disability)
 - b. non-business use, including personal messages, jokes, cartoons, or chain letter.
 - c. posting confidential information about other employees, the organisation or its customers or suppliers (this includes any statements posted from the employee's home computer and/or in the employee's own time).
 - d. online gambling
 - e. accessing offensive, obscene or indecent material, including pornography.
 - f. downloading or distributing copyright information.
 - g. sending or posting negative, abusive, rude, derogatory, or defamatory messages or statements about people or organisations, including when this is done from the employee's home (or other personal) computer and/or in their own time.
2. Any unauthorised use of email or the internet is likely to result in disciplinary action, which may include summary dismissal.

Monitoring

1. Monitoring and recording of email messages and internet use will be carried out as deemed necessary. Copies of email messages will be retained as appropriate.
2. Hard copies of email messages and details of internet sites accessed may be used as evidence in disciplinary proceedings.

Security

1. All users will be issued with (or will be asked to select) a unique individual password which will be changed at regular intervals and is confidential to the user. Access to the system using another employee's password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

Page 12 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

2. Users must take all necessary precautions against the introduction of viruses into the system.
3. Users must ensure that critical information is not stored solely within the email system. Hard copies must be kept, or information stored separately on the system. If necessary, documents must be password protected.

Implementation of the policy

1. The CEO is responsible for the implementation of the policy. This person will be available for advice on all aspects of the policy.
2. The induction programme will include training to familiarise new employees with the email system and with internet use. Managers must ensure that all new employees receive this training and are made aware of this policy and procedure prior to using email and the internet
3. This policy does not form part of the contract of employment and any or all its terms may be amended from time to time.

Social Media Policy

Policy

The organisation recognises and accepts that its employees may keep personal blogs on the internet and that internet social networking sites, such as Facebook, Twitter, Snapchat, Instagram, and WhatsApp (this list is not exhaustive) are a useful way of interacting socially with colleagues and friends. While the organisation does not wish to discourage employees from accessing such sites on the internet in their own time, nonetheless it expects certain standards of conduct to be observed to protect both its legitimate business interests and its employees from the dangers of inappropriate use. This policy applies both inside and, in certain circumstances, outside the workplace. Use of the corporate social networking site is for the purpose of sharing and disseminating information across the organisation and may be accessed at any time by authorised employees.

Procedure In the workplace / working day

1. Employees must not access personal social networking sites whilst at work
2. Authorised employees may access the corporate social networking site during working hours for business purposes only.
3. Employees may not use the organisation's corporate social networking site for personal use / blogs
4. Employees must make it clear when posting information or comments on the corporate social networking site that any personal views which are expressed do not represent those of the organisation
5. Employees must not post information on a social networking or social media site which is confidential to the organisation, its suppliers, or its customers
6. Employees must refrain from referring on a social networking/social media site to the organisation, its employees, its customers, and its suppliers

Page 13 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

7. Employees must not post entries on the corporate social networking site/a social networking site which are derogatory, defamatory, discriminatory, or offensive in any way, or which could bring the organisation into disrepute
8. Employees should be aware that blogs may create documents which the courts can order to be disclosed for use in litigation. Consequently, employees will be assumed to have written any contentious items unless they can prove definitively that they have not done so
9. The organisation will monitor its IT systems as is deemed necessary to prevent inappropriate usage
10. Hard copies of blog entries may be used in any disciplinary proceedings.

Outside the workplace

1. Employees must not refer to the organisation, its customers, or its employees on social networking/social media sites
2. Offensive, defamatory, or inappropriate comments about the organisation, its customers, suppliers, or any of its employees that employees write on social networking sites will not be tolerated
3. Employees must not make discriminatory or offensive comments about work colleagues on social networking sites
4. Employees must not divulge confidential information about, or belonging to, the organisation, its customers, or suppliers on social networking sites
5. Employees must not 'like', forward, or appear to endorse or encourage inappropriate material, blogs or posts which may bring the organisation's name into disrepute.

The above principles apply equally to information or comments posted by employees from their home (or other personal) computers and irrespective of whether the posts are done during working hours or in the employee's own personal time.

Disciplinary action

Employees whose conduct breaches this policy in any way will be subject to disciplinary action in accordance with the organisation's disciplinary procedure up to, and including, summary dismissal. Any blog entries made inside or outside the workplace that are defamatory, derogatory, or discriminatory about the organisation, its customers, suppliers, or employees will be investigated as gross misconduct. If substantiated, such conduct may lead to summary dismissal after the due process of the organisation's disciplinary procedure has been followed.

Use of Mobile Phones Policy

This organisation believes that mobile telephones used in the correct and safe manner can have a positive benefit to the operation of the organisation and to the health and safety of its employees. Use of mobile telephones in the wrong place, at the wrong time or in the wrong circumstances can cause accidents and interrupt activities to the detriment of the organisation, employees, and others. The organisation will allow the use of mobile telephones, either those provided by the organisation or an individual's own mobile

Page 14 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

telephone for personal use in emergency situations, provided the basic health and safety rules are followed.

Procedure

1. Employees must keep the use of personal mobile telephones to a minimum, i.e., very few calls and of short duration
2. Employees should avoid pressing the mobile telephone tight against the ear. They should try to hold it away from the side of the head, and alternate between left and right ear.
3. If employees have a cardiac pacemaker or other medically implanted device, they should seek medical advice before using a mobile telephone
4. Employees must not make or answer calls while driving a car on organisation business and must always exercise proper control of their vehicle. They should find a safe place to stop before answering or making a call.
5. Employees should consider the use of a hands-free set incorporating earpiece and microphone in vehicles. Otherwise, they should turn off the mobile telephone while driving or switch it to messaging.
6. Employees must not stop on the hard shoulder of a motorway to answer or make a call, except in an emergency
7. Employees should switch off their mobile telephone when at a petrol refuelling station or when near any other potentially flammable atmosphere.

Password Schedule

To keep passwords secure, R-evolution have a password schedule, this is only available to the Operations Support Manager, access to the schedule is secured by a password and is only known to these two employees. The password to the schedule is changed every 12 months. The passwords to individual systems are changed annually or when an employee who has access to a password leaves the business.

Review & Update

This policy will be reviewed and updated annually or more frequently, if necessary, to ensure that any changes to the organisation's business practices/business plan are accurately reflected.

Legal and Regulatory Requirements

UK GDPR – General Data Protection Regulation (EU) 2016/679

Data Protection Act 2018

PECR – The Privacy and Electronic Communications (EC Directive) Regulations 2003

Computer Misuse Act 1990

Page 15 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

References

ICO Guidance on UK GDPR

[https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ICO Guidance on the Data Protection Act 2018](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ICO%20Guidance%20on%20the%20Data%20Protection%20Act%202018)

[https://ico.org.uk/for-organisations/guide-to-data-protection/ICO Guidance on PECR](https://ico.org.uk/for-organisations/guide-to-data-protection/ICO%20Guidance%20on%20PECR)

<https://ico.org.uk/for-organisations/guide-to-pecr/>

Page 16 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Appendix 1 Data Protection Do's and Don'ts

Introduction

A few simple guidelines to follow best practice, protect personal data and comply with Data Protection Law.

Data Privacy

- Before using an individual's personal data, such as name, address, telephone number ensure it is lawful to do so, for example, do we have consent, a business requirement, or a legal obligation?
- Only use personal data in a way that meets an individual's reasonable expectations.
- When transferring personal data outside the organisation, ensure that it is legal to do so.
- Do not send emails, SMS, or phone individuals with marketing messages without the individual's consent.

Data Security

This policy applies to all users of computing services at R-evolution, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

- Always keep your password and username secure and do not share them.
- Do not write down passwords.
- Lock your PC/Laptop when you leave it
- Do not leave sensitive documents on your desk, file or destroy when no longer needed
- Do not open email attachments from an unknown source
- Do not download programs or run any sent by email
- Do not download any business data onto PC/laptop – use the network drives
- Ensure any personal data held on a laptop is encrypted
- If your laptop is lost or stolen contact your manager immediately.

Email Use

Using email with the following protocols will ensure safe and secure email usage:

- Before sending an email, decide whether this is the most appropriate way to communicate, for example a phone call may be an alternative
- Keep message brief and do not send any unnecessary copies of the message

Page 17 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

- When sending to a group of recipients outside the organisation, use BCC (Blind Carbon Copy) rather than CC (Carbon Copy). This will ensure that email addresses of recipients are not disclosed to each other
- Personal data, payment card data and organisation sensitive information should not be exchanged via email. If possible, select another method of data transfer or pre-encrypt the data before sending it
- Avoid forwarding emails with long message threads. Not only is this possibly annoying to the recipient, but the message threads may include information that is not intended for the recipient
- Treat external email with caution and do not click on links or download or execute attachments unless certain of source
- Staff members with access to financial assets should treat emails that request financial transfers (especially over an anonymous medium such as wire transfer) with caution. BEC (Business Email Compromise) is a method of impersonating an executive member of staff and spoofing their email identity.

Any incidence of suspicious email should be reported to the CEO.

Secure Password Tips

Keep Your System Locked ...

- Use a sensible password that is long
- Do not use a word from a dictionary
- The longer the password is the harder it is to crack
- Use a combination of lower-case, upper-case letters and numbers
- Adding a symbol will make the password harder to crack
- An easy way to remember passwords is to use a passphrase like:
Thequickbrownfoxjumpedoverthelazydog
- Add numbers 32 = Tqbfjotld32
- Add a symbol such as ? = Tqbfjotld32?

Never Use ...

- Your partner's name
- Your child's name
- Your pet's name
- Other family member's name
- Place of birth
- Favorite holiday destination
- Favorite football team
- Name of a recent film you liked
- Anything that you post on social media or use as answers to Security Questions.

Page 18 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Social Media

Be careful what you post on social media. Organisation confidential information or personal data (for example a customer’s details should not be posted).

N.B. Hackers use social media as a tool to gather information on their intended victims.

Page 19 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Appendix 2 Record Types

Statutory

Accident books, accident records/reports

- **Statutory retention period:** 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).

Accounting records

- **Statutory retention period:** 3 years following the year to which they relate.

Coronavirus Job Retention Scheme

- **Statutory retention period:** 6 years for furlough records.

First aid training

- **Statutory retention period:** 6 years after employment.

Fire warden training

- **Statutory retention period:** 6 years after employment.

Health and Safety representatives and employees' training

- **Statutory retention period:** 5 years after employment.

Income tax and NI returns, income tax records and correspondence with HMRC

- **Statutory retention period:** Not less than 3 years after the end of the tax year to which they relate.

National minimum wage records

- **Statutory retention period:** 3 years after the end of the pay reference period following the one that the records cover.

Page 20 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

Payroll wage/salary records (also overtime, bonuses, expenses)

- **Statutory retention period:** 6 years from the end of the tax year to which they relate.

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)

- **Statutory retention period:** 5 years from the date on which the tests were carried out.

Records relating to children and young adults

- **Statutory retention period:** until the child/young adult reaches the age of 21.

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)

- **Statutory retention period:** 3 years after the end of the tax year in which the maternity period ends.

Subject access request

- **Statutory retention period:** 1 year following completion of the request.

Whistleblowing documents

- **Statutory retention period:** 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.

Non-Statutory – Best Practice

CCTV footage

- **Recommended retention period:** CCTV footage may be relevant to a disciplinary matter or unfair dismissal claim. Recommended Information Commissioner's Office (ICO) retention practice is 6 months following the outcome of any formal decision or appeal.

Page 21 of 21		
Applies to: All Trustees, Employees, Trainees & Volunteers	Information Governance and Data Protection Policy and Procedure	

European Social Fund paperwork

- **Recommended retention period:** 10 years after their final ESF claim is paid by the ESF Managing Authority. 10 years after the last aid is granted under the scheme.

Inland Revenue/HMRC approvals

- **Recommended retention period:** Permanently.

Money purchase details

- **Recommended retention period:** 6 years after transfer or value taken.

Pension records

- **Recommended retention period:** 12 years after the benefit ceases.

Personnel files and training records (including formal disciplinary records and working time records)

- **Recommended retention period:** 6 years after employment ceases

Recruitment application forms and interview notes (for unsuccessful candidates)

- **Recommended retention period:** 12 months.
- **References**
- **Recommended retention period:** At least one year after the reference is given to meet the limitation period for defamation claims.

Right to work in the UK checks

- **Recommended retention period:** Home Office recommended practice is 2 years after employment ends.

Trustees' minute books

- **Recommended retention period:** Permanently.