Policy/Procedure Name:	Information Security Policy
Policy/Procedure Number:	ICT005
Date of Approval:	15 July 2011
Effective Date:	15 July 2011
Revised Date:	June 2023
Review by Date:	June 2025
Policy/Procedure Author:	Head of Technology
Policy/Procedure Owner:	Finance and Resources Director (as the Data Protection and Freedom of Information Officer and the Senior Information Risk Officer)
Management Committee Approved By:	TLT
Governor Committee (where appropriate) Approved By:	N/A
For Action By:	Staff and contractors/agency staff
For Information to:	Staff
Approval requested to upload on the Treloar's Website:	Yes □ (tick if requested)

Who is carrying out EIA?		Date of EIA?	
Have we shown due regard for the 9 protected characteristics within the policy/procedure?		Yes ☐	No ☐
Are all opportunities to promote equality taken within the policy/procedure?		Yes ☐	No ☐
Refer Policy/Procedure to EDI Co-ordinator for further assessment		Yes o	No o

1. Policy/ Procedure Aim –

This document outlines how we prevent security incidents in which the confidentiality, integrity or availability of data is compromised, and our processes if this does occur.

1.1 Scope

This policy includes in its scope all data which we process, whether in hardcopy or digital copy; this includes special category data.

This policy applies to all staff, including temporary and bank staff, and contractors.

2. Policy/Procedure Details

2.1 Policy statement

We recognise the importance of information security to our business.

Releasing data and information may have serious consequences if carried out in an inappropriate manner. To refuse to give accurate and complete data and information to those who need them, when they need them, can be equally damaging.

We will be aware of and comply with laws and regulations on data and information.

We will protect our data and information, and the data and information of those with whom we work, from unauthorised access, release or loss.

We will ensure our data and information is accurate, complete and protected from unauthorised change.

We will ensure that data and information is available on a timely basis to those who have a right of access.

We will process personal data only where we have a lawful basis for doing so. Where consent is required data will only be processed where it's "freely given, specific, informed and unambiguous".

We will respect the confidences of others so far as the law permits.

Every member of staff will take personal responsibility for supporting this policy and upholding the highest standards.

All staff who access or have management responsibility for personal and other confidential and restricted data will undergo suitable training.

Protectively marked or personal data handled on behalf of those public bodies with which we work shall be secured in accordance with guidance documents provided by those bodies.

2.2 Education and training

Every person handling information or using Treloar's information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Treloar's.

Treloar's will train all staff who handle or supervise personal and otherwise restricted data in information security.

2.3 Physical Access

- Our staff will retain personal and confidential data securely in locked storage. Access will be on a 'need to know' basis.
- Paper copies of personal information will be destroyed when they are no longer required, according to ICT003 Retention of Records policy.
- The Information Asset Register will contain the location of confidential and personal information
- Paper records should only be taken off-site where there is a necessity and not purely for convenience.
- Appendix A details the process to ensure paper records are kept safe when off-site

2.4 Digital Access

- Access will only be granted to programs necessary to complete a user's job.
- Each user will require a username and password to access information and will be trained on the use of the relevant system(s).
- Sharing of access rights is strictly forbidden.
- Staff will appropriately log out of systems after use.
- When an employee leaves their access rights will be revoked.
- Remote access via Treloar's Gateway is limited and requires MFA (see ICT001 ICT Policy for more information)
- Appendix A details the process to ensure digital records are kept safe when off-site

2.5 Data Breaches

All data breaches or near misses must be reported using the IRIS system. The Data Protection Officer will make a decision whether the breach is notifiable to the Information Commissioner's Office (Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority)* and/or to the data subject (Article 34 – *Communication of a personal data breach to the data subject*). Notification to the ICO must be made within 72 hours of our awareness of the breach. although the required information may be provided in phases as long as this is done without undue delay (Article 33(4)).

All data breaches are recorded centrally whether reported to the ICO or not.

All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer without delay.

3. Key Responsibilities

Policy/Procedure Communication and Implementation Action Plan -		
	Action	**Responsibility**
1	Ensure that all managers, employees and volunteers of Treloar's have access to the related procedures.	Treloar's Leadership Team
2	Train all managers, employees and volunteers in the implementation of the policy and the related procedures.	Human Resources Director (delegated to Training Manager)
3	Ensure that all new employees, staff and volunteers are made aware of the policy, understand it, and know where to access a copy and where to access the related procedures.	Training Manager
4	Ensure that all managers, employees and volunteers of Treloar's have access to the related procedures.	All Managers
5	Ensure that all new employees, staff and volunteers know their responsibilities, and receive training in carrying these out.	All Managers

4. Implications of Policy/Procedure

4.1 Training Requirements

Forms part of Data Protection at Induction and then refreshed annually.

4.2 Communication Requirements

How will the Policy/procedure be communicated:	Sharepoint
Who will ensure the above communication is carried out::	PA to Finance and Resources Director
Do the changes made to this policy/procedure affect any other policies/procedures? If yes, has this been communicated to the policy/procedure author/owner	No

4.3 Inclusive Communications

If you require this document in an alternative format, such as large print, audio description, or a coloured background, please contact Jo Cox at jo.cox@treloar.org.uk

4.4 Other Implementation Requirements

5. Monitoring and Review

Bi-annually

6. Links to other related policies, procedures or documents (internal)

- Policy for the use of ICT (ICT001)

7. Further sources of information (external)

- Information Management Guidance pack for Third Parties working with the Welsh Government
- Staff Handbook
- Business continuity planning

8. References

9. Revision History

Listed below is a brief audit trail, detailing amendments made to this policy procedure in last 4 years

Page/para No.	Brief description of the change(s)	Change made by	Date
all	New policy template	Jana Owens	18/05/2015
p 1	Approved by	Jana Owens	18/05/2015
2.2	Reference to section 2.2 changed to 3.2	Jane Hayden	13/04/2021
3.2	Data Protection Act 2018	Jane Hayden	20/05/2022
Various	Compliance with DSPT	Jane Hayden	28/06/23

IMPORTANT NOTES:

It is essential for those with designated responsibilities to familiarise themselves with the sources of information, referred to above.

Policy documents describe mandatory minimum standards and will be subject to audit and review. Line managers are required to ensure suitable and sufficient arrangements are in place to meet policy requirements, including the provision of information and instruction to staff.

10. Appendix A – Keeping Information Secure Off-Site

10.1 Paper Records

Paper records should only be taken off-site where there is a necessity and not purely for convenience.

If you have determined that it is a necessity to take paper records off-site, the following principles must be adopted and followed, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off-site.

- Line management approval must be obtained before personal or other confidential data contained within paper records is taken off-site. The approval request must provide details of the personal or other confidential data proposed to be taken off-site, the necessity for doing so and the relevant times.
- Only the minimum amount of data necessary for the job in hand should be removed.
- Do not leave bags or cases containing paper records visible in a car. If it is unavoidable to leave paper records in a car, eg whilst filling up with petrol, then lock them in the boot of your car. Paper records should always be secured at home at the end of your working day.
- When travelling on public transport keep the paper records close by at all times. Paper records should not be left in luggage racks or storage areas, as this increases the possibility of theft or of the item being left behind.
- Do not carry paper records 'loosely' as this increases the risk of dropping or losing them, use a file or folder to ensure they are secure
- Whilst off-site, paper records containing personal or other confidential data that are not being actively worked on must be kept secure and separate from any valuable items such as laptops.
- Paper records taken out of the office should be returned to the place of work as soon as possible, or securely destroyed if they are copies. They should not be kept out of the office for any longer than is necessary to complete the job in hand.

10.2 Digital Records

e.g memory sticks, removable hard drives etc.
All personal or confidential data that is taken off-site must be stored on an encrypted media.
There are specific offsite handsets which can be booked out from the Tech Hub in order to access eMAR and Nourish off-site – do not use the handsets from the house or classroom.