Policy/Procedure Name:	Information Security Policy
Policy/Procedure Number:	ICT005
Date of Approval:	15 July 2011
Effective Date:	15 July 2011
Revised Date:	13th April 2021
Review by Date:	April 2022
Policy/Procedure Author:	Finance and Resources Director
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 Website:	Yes □ (tick if requested)

Who is carrying out EIA?	Chief Executive	Date of EIA?	24 June 2013
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 –

To inform staff about their responsibilities with regards to information security at Treloar's

2. Introduction

2.1 Purpose

This document defines information security, states Treloar's information security policy, acts as a guide to the various documents relating to different aspects of information security at Treloar's and identifies responsibilities for information security in Treloar's.

2.2 Scope

This document covers:

- all staff, including contractors and agency workers
- all aspects of information security that are covered under the headings, as shown in section 3.2.

2.3 Background

Information security can be defined as the securing or safeguarding of all information, electronic or otherwise that is owned by an organisation.

The purpose of an information security policy is to set out how Treloar's ensures:

- Confidentiality of information – that it is accessible only to those authorised to have access.
- Integrity of information – safeguarding its accuracy and completeness.
- Availability of information – that authorised users have access to it when required.

3. Treloar's information security policy

3.1 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.

3.2 Corporate objectives to support information security

Governance, risk management and compliance
Prevent breaches of any criminal or civil law, statutory, regulatory including the Data Protection Act 1998 and the General Data Protection Regulation 2016 or contractual obligations and of any security requirements.

Evidence compliance to those with whom we work.

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.

Protective marking and asset control objectives
Ensure that access to information and other assets is correctly authorised, managed and safeguarded to an agreed and proportionate level throughout their lifecycle.

Personnel security objectives
Reduce risks of human error, theft, fraud or misuse of facilities and information.
Maintain the trust and confidence and goodwill of those who interact with and support Treloar's.

Information security and assurance objectives
Implement a management framework that will manage information security risks within acceptable tolerances.

Ensure all systems and procedures on which we rely help to assure information security objectives.

Physical security
Prevent unauthorised access, damage and interference to business assets and to restricted confidential and personal information.

Timely reviews of external threat assessments.

Business continuity
Minimise the risk of interruptions to business activities and critical business processes that enable access to information.

Ensure that processes are in place to permit the timely restoration of data following failure.

4. Key Responsibilities

Policy/Procedure Communication and Implementation Action Plan -		
	Action	**Responsibility**
1	Ensure that all managers, employees and volunteers of Treloar Trust have access to the related procedures.	Treloar 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 Trust 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

5. Implications of Policy/Procedure

5.1 Training Requirements

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

5.2 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

5.3 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

5.4 Other Implementation Requirements

6. Monitoring and Review

Bi-annually

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

- Policy for the use of ICT (ICT 01)

8. Further sources of information (external)

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

9. References

10. 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

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.