COMMUNITY SYSTEMS INFORMATION SECURITY POLICY

Last policy review date:	January 2023
Reviewed by:	Seid Almazumi
Policy publication/dissemination date:	January 2024
Next review due:	January 2024

Introduction

The confidentiality, integrity and availability of information are critical to the functioning and good governance of Community Systems. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Community Systems to recover.

This information security policy outlines Community Systems approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the 'Training Providers' information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

Community Systems is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its systems and data, including proactive measures to ensure our IT environment is built, maintained and governed in the right ways. The principles defined in this policy will be applied to all electronic information assets for which Community Systems is responsible.

Community Systems is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

Objectives

The objectives of this policy are to:

1. Provide an information security framework covering all Community Systems information systems (including but not limited to all Cloud environments commissioned or run by Community Systems, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems. It requires that:

a) The resources required to manage such systems will be made available.

b) Continuous improvement of Community Systems Information Security Management System will be undertaken.

2. Make certain that users are aware of and comply with all current and relevant UK and (where appropriate) EU or other legislation.

3. Provide the principles by which a safe and secure information systems environment can be established for staff, learners and any other authorised users.

4. Ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle.

5. Protect Community Systems from liability or damage through the misuse of its IT facilities.

6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification including upholding legal and contractual requirements around information security.

7. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

Scope

This policy is applicable to all staff, learners and third parties who interact with information held by Community Systems and the information systems used to store and process it.

This includes, but is not limited to:

- Cloud systems developed or commissioned by Community Systems,
- systems or data attached to Community System’s networks,
- systems managed by Community Systems,
- mobile devices used to connect to Community Systems networks or hold Community Systems data,
- data over which Community Systems holds the intellectual property rights,
- data over which Community Systems is the data controller or data processor (wherever held),

Policy

Information security principles

The following information security principles provide overarching governance for the security and management of information at Community Systems.

1.Information should be classified according to an appropriate level of confidentiality, integrity and in accordance with relevant legislative, regulatory and contractual requirements.

2. Users with responsibilities for information

a. ensure the classification of that information is established;
b. must handle that information in accordance with its classification level;
c. must abide by Community Systems' policies, procedures, and any contractual requirements.

3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. Access to information will be on the basis of *least privilege* and *need to know*.

5. Information will be protected against unauthorized access and processing.

6. Breaches of this policy must be reported Senior Management.

7. Information security provision and the policies that guide it will be reviewed regularly and through the use of annual external audits and penetration testing.

Compliance, Policy Awareness and Disciplinary Procedures

All new staff will receive an induction programme that covers all aspects of information security and classification of data. They are all required to sign Community Systems Data Protection Declaration prior to any access granted.

1. Compliance with this policy is mandatory for all authorised users

2. Mandatory user awareness training for all authorised users.

3. Regular audit / sampling by appointed Data Compliance Officer and external bodies.

4. All current staff will be informed of the existence of this policy and the availability of supporting policies, codes of conduct and guidelines.

5. Any security breach will be handled in accordance with all relevant Community Systems policies.

Legal & Regulatory Obligations

Community Systems has a responsibility to abide by and adhere to all current UK and (*where appropriate*) EU legislation as well as regulatory and contractual requirements.

Security Level	Definition	Examples	FOIA2000 status
1. Confidential	Normally accessible only to specified members of Community Systems staff. Should be held in an encrypted state outside Community Systems systems; may have encryption at rest requirements from providers.	1. GDPR-defined *Special Categories* of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) including as used as part of primary or secondary research; 2. patient-level observations; 3. aggregated patient data containing observations created using 5 or fewer patient-level observations; 4. passwords; 5. large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

2. Restricted	Normally accessible only to specified and / or relevant members of Community Systems staff or the student/learner body	1. GDPR-defined *Personal Data* (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs); 2. Name, email, work location, work telephone number; 3. reserved committee business; 4. draft reports, papers and minutes; 5. systems 6. internal correspondence 7. information held under licence 8. company policy and procedures (as appropriate to the subject matter)	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Public	Accessible to all members of the public	1. Annual accounts, 2. minutes of statutory and other formal committees, 3. pay scales etc. 4. Experts' Directory 5. Course information 6. Information available on the Community Systems website. 7. company policy and procedures (as appropriate to the subject matter)	Freely available on the website.