Apuldram
Centre

Information Security Policy

Version: July 2025

Version History

Date	Created by/ Amended by	Comments	Owner
Nov 2023	Rory Massey	Adopted	CEO and Operations and Compliance Manager
July 2025	Rory Massey	Reformat, restructure and reword after migration to cloud server from local server	CEO and Operations and Compliance Manager

Contents

1. Introduction

This Policy is a key component of The Apuldram Centre management framework. It sets the requirements and responsibilities for maintaining the security of information within The Apuldram Centre. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day. This policy will be emailed to staff and stored within the Organisation's Care Management System and policies documentation SharePoint site.

It applies to all staff and volunteers and should be assumed as such whenever the term 'staff' is used.

2. Aim and Scope

The aims of this Policy are to set out the rules governing the secure management of the Organisation's information assets by:

- preserving the confidentiality, integrity and availability of the business information
- ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
- ensuring an approach to security in which all members of staff fully understand their own responsibilities
- creating and maintaining within the organisation a level of awareness of the need for accurate and timely information
- detailing how to protect the information assets under the Organisation's control

This policy applies to all information/data, information systems, networks, applications, locations and staff of The Apuldram Centre or supplied under contract to it.

3. Responsibilities

The employs an external Data Protection Officer, founder of Processmatters2. They are responsible for informing and advising the Organisation and its staff on its data protection obligations. The Organisation also has an internal Data Protection Officer, the Chief Executive Officer, who is the first point of contact within the Organisation for any Data Protection matters. If a staff member has any questions or comments about the content of this policy or if theyneed further information, they should contact the internal DPO by email or telephone.

Responsibility for maintaining this Policy lies with the internal Data Protection Officer supported by the external Data Protection Officer and shall be reviewed annually.

Line Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff shall comply with this Policy and must understand their responsibilities to protect the Organisation's data.

All staff are issued with a copy of the Employee Handbook, which covers the use of IT equipment and resources, including the use of social media and the internet. All staff are required to be trained in GDPR, Cyber Security and Information Governance. Failure to comply with the requirements of the Employee Handbook and associated documentation may result in disciplinary action. Each employee is responsible for completing their own training and remaining compliant. It is the responsibility of the line manager to prompt staff to complete their training.

Line managers shall be individually responsible for the security of information within their business area.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Access to the Organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this Policy is in place. Such contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Legislation

The Apuldram Centre is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations. In particular, The Apuldram Centre is required to comply with:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

The requirement to comply with legislation shall be devolved to employees and agents of The Apuldram Centre, who may be held personally accountable for any breaches of information security for which they are responsible.

The Organisation uses the different legislation to help shape it organisaitonal policies and procuedures. It is these that the Organisation's employee must read, understand and abide by.

The requirement to comply with legislation shall be devolved to employees and agents of The Apuldram Centre, who may be held personally accountable for any breaches of information security for which they are responsible.

5. Personnel Security

a) Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.

References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity. DBS checkswill also be carried out for all staff and volunteers.

Information security expectations of staff shall be included within appropriate job definitions.

Whenever a staff member leaves the organisation their accounts will be disabled the same day they leave. The Apuldram Centre will retain access to these accounts as required for business purposes after they have been disabled.

b) Information Security Awareness and Training

The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced

An ongoing awareness programme shall be established and maintained to ensure that staff awareness of information security is maintained and updated as necessary.

c) Intellectual Property Rights

The organisation shall ensure that all software is properly licensed and approved by the CEO.

Users breaching this requirement may be subject to disciplinary action.

6. Access Management

a) Physical Access

Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

b) Identity and Passwords

Passwords must offer an adequate level of security to protect systems and data.

All passwords shall be twelve characters or longer and with other complexity such as the use of uppercase letters, lowercase letters numbers and special symbols where allowed by the individual system. Alternatively, a password could be three random words one after the other.

Where available, Multi Factor Authentication (MFA) should be used and enabled on all systems that support it.

When MFA is not available the highest complexity levels as detailed should be complied with:

All users shall use uniquely named user accounts

Generic user accounts that are used by more than one person or service shall not be used.

c) User Access

Access to information shall be based on the principle of “least privilege” and restricted to authorised users who have a business need to access the information.

d) Administrator-level Access

Administrator-level access shall only be provided to individuals with a business need who have been authorised by the CEO

A list of individuals with administrator-level access shall be held by the CEO and shall be reviewed every 6 months

Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

e) Application Access

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Authorisation to use an application shall depend on a current licence from the supplier.

f) Hardware Access

Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only.

g) System Perimeter Access (Firewalls)

The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.

The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly.

All firewalls shall be configured to block all incoming connections.

If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

h) Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed as required.

The Organisation reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

i) CCTV Access

Access to the CCTV is covered in The Apuldram Centre CCTV Policy.

7. Asset Management

a) Asset Ownership

Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

b) Asset Records and Management

An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained.

All data shall be securely wiped from all hardware before disposal. Retired IT devices are given to the Organisation's outsourced IT provider who will arrange for its destruction and will provide a certificate of destruction.

c) Removable Media

Only organisation provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded.

Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the CEO before they may be used on business systems. Such media must be scanned by anti-virus software before being used.

Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

d) Mobile Working

Where necessary, staff may use organisation-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements in line with the Organisation;'s Poratable Device Policy.

Use of mobile devices for business purposes requires a complete and authorised Portable Device Assignment Form.

Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this Policy.

All mobile devices must have their operating systems updated regularly to ensure they are running the latest security patches and updates at all times.

All signed and trusted applications downloaded onto mobile devices from verified app stores are considered approved, provided they align with the Organisation's security policies and meet Cyber Essentials requirements

Users must inform the Data Protection Officer or CEO immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

e) Social Media

Social media may only be used for business purposes by using official business social media accounts with authorisation from the CEO. Users of business social media accounts shall be duly authorised, appropriately trained and aware of the risks of sharing sensitive information via social media.

Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.

Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the organisation. If in doubt, consult the Senior Management Team.

Users breaching this requirement may be subject to disciplinary action.

8. Physical and Environmental Management

All individual offices are locked when vacant and all filing cabinets and pedestals are kept locked when not in use.

CCTV and security lighting is present throughout the site and staff are required to wear name badges.

Visitors are required to sign in and are supervised at all times.
In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security protection should be applied if necessary.

Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

9. Computer and Network Management

a) Operations Management

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the CEO.

b) System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CEO.

c) Accreditation

The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.

They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the CEO before they commence operation.

d) Software Management

All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

All software security updates/patches shall be installed within 14 days of their release as prescribed in Cyber Essentials guidelines.

Only software which has a valid business reason for its use shall be installed on devices used for business purposes including personal devices if agreed by the DPO in line with the Organisation's Portable Device Policy.

For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

e) Local Data Storage

Documents, Pictures and Desktop Folder locations should be configured for automatic backups using OneDrive and this in turn is backed up by the Acronis cloud backup platform.

f) External Cloud Services

Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider' or service provider) there must be written data sharing agreements confirming that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this Policy.

Organisational data stored on Microsoft Teams/SharePoint/OneDrive and Email in the cloud is backed up by the Acronis cloud backup platform and a random test restore of some data selected by an authorised employee will be conducted at appropriate intervals (at minimum half yearly) by submitting a ticket requesting a restore from the Organisation's IT provider.

All data/documents will be stored in line with the Organisation's Document Retention Policy. Data/documents will be removed at the required times highlighted with this Policy.

g) Protection from Malicious Software

The Organisation shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.

All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system

All anti-malware software shall be set to:

- scan files and data on the device on a daily basis
- scan files on-access
- automatically check for, and install, virus definitions and updates to the software itself on a daily basis
- block access to malicious websites

h) Remote Firewall Configuration

Following the guidelines set out in Cyber Essentials, configuration of the firewall is not permitted from the internet.

10. Response

a) Information Security Incidents

All breaches of this Policy and all other information security incidents shall be reported to the CEO and/or DPO with the Apuldram Centre Information Security Incident Policy being followed and adhered to.

If required as the result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the CEO.

Information security incidents shall be recorded in the Personal Data Breach and Information Security Incident Log and investigated by the DPO to establish their cause and impact with a view to avoiding similar events. This Policy shall be updated if required to reduce the risk of a similar incident re-occurring.

b) Business Continuity and Disaster Recovery Plans

The Organisation shall ensure that business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

c) Further Information

Further information and guidance on this Policy can be obtained from the CEO, Rory Massey, via telephone on 01243 783370 or via email on rory.massey@apuldram.org.

Comments and suggestions to improve security are always welcome.