



INFORMATION SECURITY POLICY

Record of updates

DATA PROTECTION POLICY

Date Created	October 2023	
Adopted by Trustees		
Revision Due	October 2024	
Revision Due		
Revision Due		
Revision Due		
DOCUMENT VERSION CONTROL		
Issue No.	Issue Date	Summary of Changes
1	October 2023	Original Draft Policy from One West

Introduction

The RISE Trust is responsible for the control of a number of individuals' Personal Data (PD) including staff, trustees, families, children and young people, and a number of other individuals who interact with The RISE Trust. In addition to PD, information that may be considered of a sensitive nature will include financial records, planning and management forecasts, and risk assessments, which also require appropriate security applications to be made and are included within the scope of this policy.

The Information Security Policy (ISP) is designed to inform employees of the appropriate principles and methods to create, store, secure and, dispose of information in all formats to ensure security is of a consistently high standard. Compliance with this Policy provides management, staff, and associated individuals with:

- Assurance that information is being managed securely in a consistent and effective way.
- Assurance that The RISE Trust is able to provide a trusted environment in which to handle information as part of its activities.
- Clarity regarding the individual responsibilities for Information Security.
- Demonstration of best practice.
- Assurance that information may only be accessed by those authorised to have access.

Scope

This policy applies to all employees of The RISE Trust including contract, agency and temporary staff, volunteers and employees of partner organisations working with or for The RISE Trust.

The ISP can be used by employees who use data as part of their day-to-day business, those who manage and administer data and by those responsible for the management of data storage systems.

Aim

The ISP aims to ensure that all employees are aware of the following principles of the CIA Triad when dealing with information and use the principles from their day-to-day handling of information up to the development and adoption of new ways and systems designed for handling information. These principles will also help The RISE Trust comply with Article 32 of the UK GDPR which refers to adequate organisational and technical security;

Confidentiality: Information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity: Maintain the accuracy and completeness of data over its lifecycle.

Availability: Information must be available when needed and appropriate means of access or disclosure must be understood.

In addition to the protection and maintenance of the confidentiality, integrity, and access of data this policy will support the trust to meet the following:

- manage the risk of security exposure or compromise.
- assure a secure and stable information technology (IT) environment.
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
- monitor systems for anomalies that might indicate compromise, and
- promote and increase the awareness of information security.

Adoption of this concept will reduce the risk of harm to individuals, reduce the vulnerability of the trust, and the likelihood of financial penalties that may be given by supervisory authorities such as the Information Commissioner's Office (ICO).

Roles and Responsibilities

Information Security Lead Accountability for Information Security rests with the Information Security lead who is the CEO. The Information Security Lead may discharge this function to members of the senior leadership team (SLT) or another responsible individual to carry out the activities of Information Security.

Such activities may include.

- Evaluating and accepting risk on behalf of The RISE Trust.
- Identifying information security responsibilities and goals and integrating them into relevant processes.

- Supporting the consistent implementation of information security related policies and processes.
- Supporting security through clear direction and demonstrated commitment of appropriate resources.
- Promoting awareness of information security best practices through the regular dissemination of relevant material such as that provided by the Data Protection Officer (DPO).
- Implementing the process for determining information classification and categorisation, based on recommended practices, and legal and regulatory requirements, and to determine the appropriate levels of protection for that information.
- Implementing the process for information asset identification and recording them in the Record of Processing Activities (RoPA) as well as the handling, use, transmission, and disposal based on information classification and categorisation.
- Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.
- Participating in the response to security incidents.
- Complying with notification requirements in the event of a breach of personal data.
- Adhering to specific legal and regulatory requirements related to information security.
- Communicating legal and regulatory requirements to the ISO/designated security representative, specifically article 32 of the UK GDPR (Security of Processing).
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.
- The development and implementation of new technologies to build safe and secure systems.

Governance of Information Security may be formalised to include a regular review and working group to identify business requirements and how they impact existing information use and future use.

Data Protection Officer (DPO) The DPO, i-West, is responsible for monitoring The RISE Trust's compliance with Data Protection legislation. This is completed by the following means: an annual assurance review; breach and security incident monitoring; and review and providing sufficient guidance to the Information Security Lead for them to carry out their task where PD may be processed.

The DPO will support The RISE Trust in the event of any breach of information where it relates to personal data.

Managers/Senior Staff Primarily responsible for ensuring the security of the systems that hold data and the physical environments where information is processed or stored. They are also responsible for the following:

- Ensuring all employees within their area of work are aware of the relevant policies applicable to their role i.e. Acceptable Use Policy, Confidentiality agreements, Bring Your Own Device (BYOD) guidelines and eSafety.
- Determining and controlling the access levels of employees and relaying that information, including when access must be removed, to the CEO or individual responsible for the control of electronic access.
- The control of passwords, keys, combination lock numbers or any other physical form of access control within their area of work.
- Ensuring that employees have taken part in the relevant and adequate training in a timely manner.
- Making employees aware of security breaches or threats and translating points learnt from such incidents into working practices.

CEO - IT Lead The CEO is the individual responsible for management of IT whether on-site or through a third-party contract must ensure that.

- All network, mobile devices, and removable media assets are securely controlled and managed. This includes maintaining appropriate storage facilities, producing, and reviewing guidance regarding the safe storage and use of assets, user access agreements and user access control, such as the removal of users when informed to do so by managers, or under exceptional circumstance.
- The maintenance of software in use by the trust. This includes software patching routines, application or alterations or the removal of software considered to be vulnerable, the assessment of such levels of vulnerability, and the notification to all relevant staff of existing threats, emergent threats, and appropriate safe use. This information may be provided to managers in support of their responsibilities for awareness.

Information Owners/Responsible Persons The approach to the use of data will determine who Information Owners are. In general, the ownership or responsibility will fall to the relevant manager, or person who retains and uses the information within their workspace, for example the Designated Safeguarding Lead (DSL) will own Safeguarding Information; and individual outreach workers will own client lists and family information where it is not held on The RISE Trust SharePoint.

It is good practice to record the relevant owner or responsible person so that any issue regarding the use, management or breaches of that information may be brought to their and the DPO's attention. This is referred to as an Information Asset List, however it may be incorporated into the Record of Processing Activities (RoPA) used for Data Protection purposes.

Information Owners will be responsible for managing the accuracy and security of their data. This will mean that their relationship with their peers and managers should be open and transparent.

Owners will also need to discuss with the Information Security Lead and DPO the implications of using third parties to process information or when sharing information. Where this includes PD or other sensitive information, appropriate agreements must be in place.

All Employees and External Individuals Everyone is responsible for Information Security and should be aware of and understand the requirements of on them in line with this Policy and any associated guidance.

The key points for all employees to remember are:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted to them.
- Protecting information and resources from unauthorised use or disclosure.
- Protecting personal, private, sensitive information from unauthorised use or disclosure.
- Abiding by policy and guidance related to information security such as e-Safety, Acceptable Use, confidentiality agreements and the conditions of use of any device issued by The RISE Trust.
- Reporting suspected information security incidents or weaknesses to the appropriate manager.

Individuals who may work in The RISE Trust with information but not be an employee, such as IT technicians, auditors or external agencies, should be able to demonstrate their organisation's Information Security approach or have an appropriate confidentiality statement within their work description.

They should be made aware of what they should do if they inadvertently access information that they should not have done or discover a breach. This may be as simple as letting them know to contact the person who is responsible for them or making them aware of who the relevant manager is that they can report to.

Areas That Require Specific Adoption of Information Security

Contracts of Employment Staff suitability must be assessed at all points of employment, in line with safer recruitment policies and guidance, and all employee contracts must contain reference to confidentiality. Information in the form of the Acceptable Use Policy, Data Protection Policy or specific confidentiality guidance must be provided to employees at the appropriate time.

Control of Information Access Information shall be restricted to only those who have an acceptable business reason to access such information.

Information Owners/Responsible Persons must be consulted before access is granted or an appropriate process of access must be in place.

Passwords or emergency access without authorisation may only be made in exceptional circumstances and the decision to do so must be relayed to the relevant Information Owner, Manager, or the Information Security Lead at the earliest possible point.

Staff Owned Devices

- See The RISE Trust Bring Your Own Device Policy

Computer Access Controls Access to computer systems must be managed by IT or the person responsible for IT. This may be by active directory or, in the case of portable devices, by providing a temporary password.

There must be a form of system monitoring that can be used to determine who accessed which device and at what time, at a basic level this may be using Active Directory, Event Viewer, or a more complex User activity Monitor (UAM) software.

The fundamentals of password security are required to ensure that passwords are not shared which would result in misidentification with the exception of the point regarding emergency access in the previous paragraph.

Application Access Controls Specific applications must be administered effectively by either IT or the responsible person for any third-party application, such as Tapestry. This is particularly relevant for The RISE Trust SharePoint; however, this applies to all other applications where it has been deemed that access controls are required.

When adopting a new application, a proper assessment of access controls must be made and, if necessary, locally produced guidelines regarding its use should be made. This may be covered as part of a Data Protection Impact Assessment.

Equipment Security Information may be stored in physical containers such as filing cabinets, draws, safes and storage rooms. It will in most cases be retained electronically, however the principles of security are the same.

Any area where information is stored must be secured in a manner appropriate to the type and sensitivity of information stored within, for example sensitive financial records, safeguarding records and HR records must be secured by lock, or if stored electronically on a secure section of the SharePoint network isolated by specific permissions.

General lists and necessary contact details should be stored out of sight in line with a clear desk routine, or, if stored electronically, may be stored in a general open section of the computer network.

Information Owners must assess the level of security required and where necessary consult with the Information Security Lead/ CEO. In cases where highly sensitive information is stored electronically, it should be encrypted wherever possible.

Computer Network Procedures The arrangement and control of the computer network should be documented and must not remain with a single person. The reliance upon a sole individual's understanding of the system can undermine the principle of availability, if they leave or are unavailable, due to the potential loss of access, and may lead to loss of data if a full understanding of the type and location of data is not retained.

Information Security Breaches and Reporting Any breaches of information security must be reported to the Information Security Lead and, where it involves the inappropriate access via hacking, malicious attack, lack of security around an electronic system, loss of physical device or any other similar situation, IT must also be informed.

In instances where there is the potential breach of PD the DPO must also be informed at the earliest possible point.

The confidentiality or security of information that has been breached which was held in a physical format, i.e. paper record, application form or folder, does not need to be reported to IT in most circumstances, however the Information Security Lead must still be informed.

Protection from Malicious Software The RISE Trust and its IT providers shall use software protection to detect and deny intrusion, email filtering and if possible, adopt measures such as SPF, DKIM and DMARC (to stop the trust's email addresses getting spoofed). Users should not be able to install software on The RISE Trust's network without prior approval or introduce malicious software via other routes, i.e. the use of unmanaged USB devices.

The CEO should have a documented process for Cyber Security, seek formal accreditation of IT processes, or adopt standards that equate to accreditation.

Removable Media Any removable media should be supplied and managed by the trust and controlled effectively by the use of an asset register. The Register should contain who has which device, when it was issued and who issued it. Frequent auditing of issued devices should take place in order to identify any unknown losses. USB port access should, if possible, be restricted either fully or to a select computer, user, or managed device. This includes The RISE Trust mobile phones – personal phones should NOT be charged on a RISE laptop.

Any external information device that someone wishes to use should be submitted to their manager and IT for approval prior to use although this will only be allowed in exceptional circumstances. Where PD or information of a sensitive nature may be stored, encryption must be applied to removable media devices.

USB drives are not allowed to be used at The RISE Trust.

Monitoring System Access and Use Systems should, where possible, be adopted that can provide an auditable trail of access, this is considerably more important as the type and sensitivity, or the information being accessed increases. In terms of physical records, this may be limitation to a single or small number of individuals or a signing in and out form, this may be particularly applicable to records that contain special categories of personal data.

Electronic systems will, in many cases, have event record logs, however the trust must ensure that they understand how this function works and how it may be used when required, or, if it is inadequate, be able to work with the CEO or IT provider to apply any additional software as necessary.

The RISE Trust must make it clear to employees that information contained on the trust's system is subject to access and monitoring and that, except in exceptional or agreed circumstances, should not be used for personal reasons by employees. The limitations of this may be defined in the Acceptable Use Policy, contract terms or specific guidelines created for this purpose.

Accreditation and Assessment of Systems The Information Security Lead must be assured that new systems, be they physical or electronic, are adequately assessed by the relevant manager, CEO or responsible person.

Such assessment may not need to be formally documented but demonstration of the assessment must be recorded appropriately. Recognised accreditation will provide a significant level of assurance; however, it must be taken into account with the intended way of using any application.

System Control Change Any change made to any system must be confirmed with the Information Owners and, where any conflict arises, must be referred to the Information Security Lead. Access abilities to alter any system parameters should adhere to the Principle of Least Privilege.

Business Continuity and Disaster Recovery Plans The Information Security Lead is responsible for ensuring that, in the event of any catastrophic failure of a system, there is adequate capability for the continuation of the use of information in line with the CIA Triad. Any system which is deemed to be critical to The RISE Trust should be included within a Business Continuity Plan, this may include The RISE Trust SharePoint, access to financial resources or safeguarding information.

Cyber Incident Response Plans (CIRP) should be adopted and tested. A CIRP may form part of a disaster recovery plan but should be separately identifiable within that plan.

Training and Awareness Information security may not be considered a separate training topic in its own right; however, the CIA Triad should underpin any training in relation to the processing of data. This will include system use and operation, data protection training, safeguarding, and procurement training.

Document Classification

The adoption of a document classification system may be used to determine the appropriate level of security that should be applied to data that is held by the trust. It may not be a possibility to mark individual documents with a protective marker, however, an understanding of the sensitivity of the information, particularly in relation to those identified in section 5, must determine the handling of data.

A determination of what data constitutes a higher risk may be derived from tools such as the Record of Processing Activities (RoPA), Information Asset Registers or localised guidance. Where a system is not partitioned or does not have controls to allow any alteration of security measures, it must be considered to be at the level required by the most sensitive information held.

An example of this may occur where a financial system is used to manage queries as well as hold account specific data, in the case the queries would be require a relatively low level of security whereas the account specific data will require considerably more security.

As shown the data held in a system may not need to be marked, or may not be able to be marked, however when moving data outside of that boundary it should be adequately controlled, i.e. a print out of on-going safeguarding incidents has been removed from the security of its system, in this case it may be necessary to mark the records as confidential and include the name of the owner to whom they may be returned if misplaced.

Levels of classification may be developed to meet The RISE Trust's specific requirements:

Protective Marker	Caveat	Covers
Unmarked	None	General information, trust updates, public information, newsletters etc. <ul style="list-style-type: none"> RISE Directory
Confidential	Safeguarding, HR/Personnel,	Generally, information that relates to a person or may be considered personal data which was provided in confidence or may have been discussed without the intention of disclosing it to an individual or individuals. <ul style="list-style-type: none"> Outreach Human resources Accounts Management Volunteering Courses Contact Centre Rise preschools Administration Admin accounts only Trustees

Sensitive	Finance, HR, Planning, Policy, Contracts	<p>This will cover information that may cause disruption to The RISE Trust business if inadvertently disclosed.</p> <ul style="list-style-type: none"> • Accounts • Management • Human Resources • Ofsted • Trustees • Admin accounts only
-----------	--	--

The key principles of data classification and handling are.

- All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business; this should be defined in the RoPA.
- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information should be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- If The RISE Trust is unable to determine the confidentiality classification of information or the information is personal data, the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- The RISE Trust must communicate the requirements for secure handling of information to its workforce.
- A written or electronic inventory of all information assets must be maintained. The RoPA will meet this requirement for personal data, however business sensitive information may necessitate an additional register.
- Content made available to the general public must be reviewed according to a process that will be defined and approved by The RISE Trust. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- Personal data must not be made available without appropriate safeguards approved by The RISE Trust.
- For non-public information to be released outside The RISE Trust or shared between other entities, a process must be established that, at a minimum:

1. Evaluates and documents the sensitivity of the information to be released or shared.
2. Identifies the responsibilities of each party for protecting the information.
3. Defines the minimum controls required to transmit and use the information.
4. Records the measures that each party has in place to protect the information.
5. Defines a method for compliance measurement.
6. Provides a signoff procedure for each party to accept responsibilities; and establishes a schedule and procedure for reviewing the controls.

Associated Policy and Guidance

- Data Protection Policy
- Acceptable Use Policy
- Bring Your Own Device Policy