Sheffield Institute of Education Research and Knowledge Exchange Information Governance Statement

|  |  |
| --- | --- |
| Effective from | September 2023 |
| Planned Review Date | June 2024 |
| Version | V 2023.1 |
| Enquiries to | Prof. Emily Perry, Head of SIRKE e.perry@shu.ac.uk  |

# Introduction

* 1. This document sets out the information governance and data security measures that Sheffield Institute of Education Research and Knowledge Exchange Centre (SIRKE) has in place to process personal data and other confidential data.
	2. SIRKE is a Sheffield Hallam University [research & knowledge exchange (RKE) centre](https://www.shu.ac.uk/sheffield-institute-education-research) that is supported by central University directorates which supply services such as IT, HR, facilities and estates and central University governance structures.
	3. SIRKE is part of Sheffield Institute of Education (SIOE), which also includes the SIOE Teaching Department. Staff involved in research and knowledge exchange projects in education are based in SIRKE, the Department, and sometimes from other areas of the university. This information governance statement covers all staff involved in research and knowledge exchange projects; these staff are aware of and adhere to this governance statement.

# Compliance

* 1. Sheffield Hallam University is registered as a Data Controller in accordance with The Data Protection (Charges and Information) Regulations 2018. The University is registered as SHEFFIELD HALLAM UNIVERSITY HIGHER EDUCATION CORPORATION (Registration Number: Z6559086). The register entry can be viewed on the Information Commissioner's [website](https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/):

The University is also a public authority for the purposes of the Freedom of Information Act 2000.

* 1. The University ensures that all personal information is handled in accordance with Data Protection legislation.
* Systems and services handling this information are compliant
* Staff handling personal information are aware of their responsibilities
* The University ensures that any contractors or sub-contractors are also compliant with the requirements of the Data Protection legislation and other relevant legislation
	1. The University has an [Information Governance Policy](https://www.shu.ac.uk/about-this-website/privacy-policy/information-governance-policy), a policy on the use of special category personal data and criminal offence data, an Encryption policy and a Monitoring Policy as well as IT regulations and policies, security policies, financial regulation and policies and HR policies.
	2. The University has a Data Protection Officer (DPO) whose qualifications include the ISEB/BCS Practitioner Certificate in Data Protection (updated for GDPR) and Freedom of Information.
	3. SIRKE staff and all other staff working on RKE projects in education are aware of and adhere to the [University's Information Governance Policy](https://www.shu.ac.uk/about-this-website/privacy-policy/information-governance-policy).
	4. All staff are aware of the security reporting structure and report all security incidents, physical or electronic, to the relevant contact.
	5. This statement is reviewed annually to ensure that it is accurate, up to date, and reflects current legal, regulatory, and contractual requirements. 
	6. SHU’s Information Governance Structure can be seen in the diagram below:

**

# Personnel Security

## Recruitment, Selection and Vetting of Staff

* 1. Sheffield Hallam University recruitment and selection policies and processes ensure that appropriate checks are made on all staff who have access to personal and confidential data. This is also the case for IT staff who administer and maintain the University's IT network and facilities.

These include:

* Identity validation
* Verification of qualifications
* Employment history
* Nationality and Immigration Status
* Criminal record (self-declaration for unspent convictions)
* Where appropriate and where permitted by the Rehabilitation of Offenders Act 1974 and the Police Act 1997, SIRKE staff are also DBS checked

# Staff Contracts and Confidentiality Arrangements

* 1. The University's standard terms and conditions of employment include requirements not to misuse or inappropriately disclose any confidential information which may be obtained during the course of employment, or by having privileged access to systems and data, or a specific security role or responsibility. The requirement to maintain confidentiality continues after a member of staff has left the University.

## Staff Induction and Training

* 1. All University staff are expected to complete an induction programme. This is mandatory for all SIRKE staff and includes information about:
* Their security responsibilities
* Their legal responsibilities, in respect of:
	+ The General Data Protection Regulation and the Data Protection Act 2018
	+ Freedom of Information Act 2000
* SHU’s IT regulations
* How to recognise a data security incident
* How to report a data security incident
* Completion of a *Cyber Awareness* module
	1. All staff are familiar with the University's [Data Encryption Policy](https://eisf.shu.ac.uk/EISF2015/ElectronicDataEncryption.html).
	2. Staff are made aware that a breach of data protection legislation is potentially a disciplinary issue.
	3. Development and training requirements are agreed through the SHU Performance and Development Review (PDR) process. All SIRKE staff receive mandatory annual information governance refresher training. Attendance is logged.

## Staff Access to Data and Information

* 1. Staff access to personal and confidential information is in line with project privacy notices and university privacy notices for [staff](https://www.shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-staff), [students](https://www.shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-students) and RKE. Data will not be kept any longer than is necessary and in line with contractual obligations and GDPR.
	2. Access to personal and confidential information is similarly restricted and controlled.

## Staff Movers and Leavers

* 1. Account access is updated when a member of staff moves to different roles.
	2. The University has a checklist for staff leavers and movers and for their line managers to manage records and information assets during their notice period.

# Security of the Physical Environment

## Campus and Building Security

* 1. SIRKE’s base is the Arundel Building at Sheffield Hallam University’s city campus.
	2. Card access to SIRKE offices within the Arundel building is restricted by access control and is periodically reviewed by the Research and KE Manager. All card access is recorded so, in the event of a security incident or concerns about access, an audit trail of access over a period of time can be produced and checked.
	3. Visitors are permitted by an intercom system.
	4. Access to Arundel level 1 is by electronic staff card (SHU Card). SHU Card Access rights are managed by the University's Security Team. SHU Cards are returned when staff leave the University and associated access rights are terminated. In addition the staff offices and store room on Level 1 all have an additional access control feature. For visitors the outer door on Arundel Level 1 also has a video doorbell that rings through the Research Centre’s phone system, you can see who is at the door before granting access.
	5. The Facilities Directorate provides a University security service 24 hours a day 365 days a year with staff who patrol the campus and a control room which handles calls from staff. CCTV cameras are also in place across the campus.

## Office Security

* 1. Computers are locked (requiring a password to unlock) when not in use or left unattended.
	2. Paper records containing confidential or personal data are not left unattended on desks and are returned to locked storage when not in use.
	3. USBs and all other portable storage devices are also locked away when not in use and are not left unattended.
	4. Laptops and other mobile computers are securely stored when not in use. All Managed Desktop laptops use Bitlocker drive encryption in order to protect data on the C: drive.
	5. All documents are physically released at the printer by use of an access token (SHUCard) or password.
	6. Paper records containing personal or confidential data are either shredded and/or disposed of in the University's confidential waste system when they are no longer needed.

## Fieldwork and Working Off-site

* 1. When staff work outside of their offices, they adhere to the [Information Security Policy](https://eisf.shu.ac.uk/EISF2015/RelatedUniversityGuidance.html) for Staff Who Work Off-Campus and undertake measures to ensure compliance with data protection legislation.
	2. Portable devices used to collect, store and process personal data are encrypted or stored using alternative data secure measures.
	3. Data collected off-campus on portable devices is transferred to the N:, Q: or J: drive as soon as possible to ensure that it is backed up on the University's IT network. It is then removed from the portable device.
	4. All laptop computers have access control, equivalent to that used on the University's desktop PCs. Laptop computers have anti-virus measures installed and are encrypted to at least a minimum of FIPS 140-2.
	5. If working from home, staff use a secure VPN/remote desktop to access files and confidential information.

# Access Control

* 1. Staff are only given access to personal and confidential information if there is a legitimate business requirement for them to have access to this information and in accordance with the terms of the relevant contract.
	2. Staff, once provided with access, will only access personal and confidential data when there is a legitimate business need to do so.

## Access to IT facilities and electronic data

* 1. All staff are given access to IT facilities according to the University's [Access Control and Account Management Policy](https://eisf.shu.ac.uk/pdf/AccessControlandAccountManagementPolicy.pdf).
	2. All staff have individual IT accounts, for privacy and accountability.
	3. All IT users are bound by the [Regulations for the use of IT Facilities](https://eisf.shu.ac.uk/EISF2015/RegulationsForTheUseOfITRegs.html) and the [JANET Acceptable Use](https://community.jisc.ac.uk/library/acceptable-use-policy) Policy.
	4. Users are not permitted to allow any other person to access any system with their login details or system permissions.
	5. Users are not permitted to use the login details of another user or to attempt to access any systems or data for which they have not been granted permission.
	6. Staff must notify their manager if they have been provided access to confidential files that they do not require access to.

# Electronic and Network Security

* 1. All hardware used to process confidential information is regularly maintained and is installed with up-to-date anti-viral software and firewall protection.
	2. Data is backed up every night to a central backup system. Access to the system is restricted to IT staff concerned with operation of the backups. Data in the backup system is deduplicated or compressed while stored.
	3. The disposal of hardware is completed in accordance with the University's [Disposal of IT Equipment Policy.](https://eisf.shu.ac.uk/EISF2015/DisposalofIT.html)
	4. All staff adhere to the University's [Password Policy](https://eisf.shu.ac.uk/EISF2015/PasswordPolicy.html). The requirement in SIRKE is for passwords to be changed regularly.
	5. Passwords should not be shared with anyone or written down in an area which is easily accessible.
	6. All new networks are secured before data processing begins.
	7. When transferring confidential or personal data; all staff adhere to the University's [Electronic Data Encryption Policy](https://eisf.shu.ac.uk/EISF2015/ElectronicDataEncryption.html), and ensure a minimum encryption of FIPS 140-2 for mobile computers and removable storage (including, but not exclusively: hard drives, USBs and CDs), in-line with guidance from the Information Commissioner's Office.

# Data Security Breach Management

* 1. The University has a [Data Security Breach Management Procedure](https://eisf.shu.ac.uk/EISF2015/ManagingInformationSecurityIncidents.html) to manage data breaches relating to personal data. The policy states that it is the responsibility of all staff to report an incident or a near miss/close call immediately, ensuring compliance with the 72 hour deadline in which suspected data breaches should be reporting to the Information Commissioners Office (ICO). Staff are aware of this requirement.
	2. A data security breach is defined as, "an event or series of events leading to the unintentional or unauthorised disclosure of information which compromises the security, confidentiality or integrity of data".
	3. The Procedure also requires staff to report near misses or close calls. These are defined as, "incidents which did not result in the loss or theft of personal data, but had the potential to do so and where there is the possibility of a future breach, either because there is a weakness in a policy or process or a vulnerability in a system".
	4. IT security incidents must be reported to IT Help.
	5. Incidents and concerns relating to the physical security of staff and premises must be reported to University's Security Team.
	6. Staff are aware of the security reporting structure below and report incidents to the Head of SIRKE.



# Information Asset Management

* 1. The University has a central asset register which incorporates the requirements of Article 30 of the GDPR.
	2. All information assets are recorded on the SIRKE Information Asset register which feeds through to the central asset register.
	3. Information Asset Registers (IARs) are regularly reviewed and updated.
	4. Retention periods are noted for each information asset as it is recorded on the SIRKE Asset Register. This covers all personal data, both project and non-project related.
	5. Information assets are deleted or securely destroyed at the end of the retention period.
	6. The IAR outlines what data will be archived at the end of the programme.

# Physical Assets

* 1. For hardware purchased by central IT services, SIRKE maintain a separate physical asset register which logs who is allocated a piece of equipment.
	2. Staff are briefed on how to keep physical assets and information which is stored on them secure.

# Organisational-wide Data Protection Compliance Statement

The following is the current Sheffield Hallam University Information Governance and IT Security Statement:

# INFORMATION GOVERNANCE AND IT SECURITY STATEMENT

## INTRODUCTION

The University has a strong culture of information governance compliance and information security and relies on being able to manage a broad range of personal, confidential or sensitive data safely and effectively. The University uses appropriate strategy and policy to ensure that information is handled and processed securely in the course of its business.

Ultimate responsibility for information governance and information security is held by the Board of Governors through the work of the University Audit and Risk Committee. The Deputy Vice-Chancellor (Strategy & Operations) has been appointed as the University Senior Information Risk Owner (SIRO). Day-to-day responsibility for IT security strategy and operations is delegated to the Chief Information Officer and Digital Technology Services (DTS) who have a standing security team of four, responsible for security operations and management. Information Governance is the responsibility of the University Secretary and Head of Information Governance who is the University’s Data Protection Officer (DPO) and leads a team of two Information Governance Officers.



## INFORMATION GOVERNANCE COMPLIANCE

The University and, where required, its wholly owned subsidiary companies, are registered with the Information Commissioner's Office (ICO).

Sheffield Hallam Higher Education Corporation – registration number Z6559086

Sheffield Hallam University Enterprises Limited – registration number Z6912522

SHU Law Limited – registration number ZA487596

The University is a public authority as defined by the Freedom of Information Act 2000 and the Data Protection Act 2018. The University has appointed a Data Protection Officer (DPO) in line with legal requirements for public authorities and the DPO has registered with the ICO. The University’s DPO is Helen Williamson (DPO@shu.ac.uk). The DPO and the Information Governance Team work with local Information Governance Guardians across the University to ensure compliance is embedded in all areas of processing. These Guardians meet quarterly at Information Governance Forums. The DPO makes regular reports to the Senior Information Risk Owner (SIRO) who is the Deputy Vice-Chancellor (Strategy & Operations) and a member of the University’s Leadership Team.

The University has an [Information Governance Policy](https://www.shu.ac.uk/about-this-website/privacy-policy/information-governance-policy) and a policy on the processing of special category personal data and criminal offences data in accordance with the requirements of Schedule 1, Part 2, Paragraph 5 and Schedule 1 Part 4 of the Data Protection Act 2018. In addition, the University has a Monitoring Policy, a procedure for managing data security incidents and breaches and a range of guidance for staff and students.

The University has compiled an Information Asset Register to meet our duties to maintain records of processing activities. Maintenance of the Information Asset Register managed by the Information Governance team.

The University has introduced standard checks for suppliers who act as data processors and has standard contract clauses, data sharing agreements and data processing agreements in place. A process for conducting Data Protection Impact Assessments is in place.

The University has a bespoke e-learning module for data protection and the Information Governance team also provides a range of face-to-face data protection training. The Information Governance Team works with academic departments and professional services directorates to target ongoing awareness raising activities, training, updates and reminders to staff and students. A suite of corporate [privacy notices](https://www.shu.ac.uk/about-this-website/privacy-policy) has been developed for the University’s stakeholders. The privacy notices are published on our website and are reviewed and updated regularly. Information about data subject rights is also available on our website and in our privacy notices. Requests from data subjects in relation to their data protection rights are managed via the Information Governance Team and cascaded via a network of local contacts.

The same network of local contacts is used for managing requests under the Freedom of Information Act and the Environmental Information Regulations. The University’s Publication Scheme together with schemes for all wholly owned subsidiary companies can be found on our [website](https://www.shu.ac.uk/about-this-website/freedom-of-information#this-section).

## INFORMATION SECURITY

The University follows the NCSC ‘10 Steps to Cyber Security’ framework to structure security planning and operations. Through information strategy, policy and process the University is aligning to the ISO27001 standard. Alongside this the University is introducing an ISO20000 aligned Service Management strategy for IT services, elements of which support development of information security.

The University has a Cyber Essentials certificate covering specific networks that are used by staff requiring the Cyber Essentials standard.

The University understands that information security is a continually evolving area and management and governance is designed to ensure that it can adapt easily to new threats, risks and requirements. There is a collection of regularly reviewed information security policies to underpin governance are publicly available through the University IT Security Policies, Procedures and Related Guidance web site (see [https://eisf.shu.ac.uk](https://eisf.shu.ac.uk/)).

In addition, all use of University IT systems and services is covered by the [Regulations for the Use of IT Facilities](https://eisf.shu.ac.uk/EISF2015/RegulationsForTheUseOfITRegs.html).

These policies and regulations form the basis of the Information Security Management processes in the University, developed to align with ISO20000 and regularly tested through response exercises.