The
Sir John Brunner
Foundation

INFORMATION SECTURITY POLICY

APRIL 2025

Excellence I Belonging I Partnership

Document Control Sheet

Document Type	Policy
Document name	Information Security Policy
Originator	Chief Financial & Operations Officer
Approved by	Foundation Board
Date approved	02 April 2025
Review interval	Biennial
Date of last approval	New Policy
Date of next review	March 2027
Equality Act 2010 issues fully considered	Considered to be neutral.
Associated Policies and Procedures	Data Protection Policy Records Management Policy

The Sir John Brunner Foundation
Northwich, Cheshire, CW9 8AF Tel: 01606 664900

INFORMATION SECURITY POLICY

1 Rationale

1.1 The Sir John Brunner Foundation needs to obtain, process and store certain information about its employees, students and other users to both operate and meet its legal and contractual obligations. The purpose of the Information Security Policy is to ensure business continuity, to minimise operational damage by reducing the impact of information security incidents and to ensure compliance with relevant legislation including the Data Protection Act 2018 and UK GDPR.

2 Scope of the Policy

2.1 The Information Security Policy applies in respect of all I.T-related systems, hardware, services, facilities and processes owned or otherwise made available by the Foundation or on its behalf, or which are connected to the Foundation network and servers, including for the avoidance of doubt any personally-owned devices that are used in connection with Foundation activities (together, I.T. Systems).

3 Status of the Policy

3.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that colleagues will abide by the rules and policies made by the Foundation from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

4 Definitions

4.1 **Special category data** is:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person’s sex life; and
- data concerning a person’s sexual orientation

4.2 **Confidential information** refers to any data or knowledge that is shared with an individual or organisation under the condition that it remains private and undisclosed.

4.3 **Foundation**. For the purposes of this policy, the term "foundation" refers to all Sir John Brunner Foundation academies and central teams.

5 Risks

5.1 The Foundation is facing increasing security threats from a wide range of sources. Systems and networks may be the target of a variety of attacks, including computer-based fraud, surveillance or vandalism. Such threats to information security are generally expected to become more widespread, more ambitious and increasingly sophisticated.

5.2 Due to increasing dependence on I.T. systems and services, the Foundation is becoming more vulnerable to information security threats. The growth of networking, cloud services and mobile devices presents new opportunities for unauthorised access to computer systems or data and reduces the scope for central, specialised control of I.T. facilities.

5.3 In addition, legislation has been introduced, which places legal requirements on the Foundation to protect personal privacy and to ensure the confidentiality and security of information and that its use is within the law.

6 Compliance Responsibilities

6.1 The Foundation sets out the responsibilities of anyone using I.T. Systems and these are included in the relevant academy Staff and Student Handbooks.

This Policy supports and expands on the provisions in the IT Acceptable Use regulations governing the use of computing and IT facilities and follows DfE guidance. All members of the Foundation, including staff, students, governance and any other user with access to Foundation I.T. Systems, must comply with this Information Security Policy.

7 Information Handling

7.1 **Classification of information**

An inventory will be maintained of all the Foundation's major I.T. assets and the ownership of each asset will be clearly stated. Within the inventory, the information processed by each I.T. asset will be classified according to sensitivity.

7.2 Precautions against hardware, software or data loss

Equipment must be safeguarded appropriately, especially when left unattended. Files downloaded from the internet, including files attached and links within emails, must be treated with caution to safeguard against Phishing type attacks for both malicious code and the harvesting of personal information.

7.3 Disposal of equipment

When permanently disposing of equipment containing all types of storage media (including removable media), all special category or confidential data and licensed software should be irretrievably deleted during the disposal process. Damaged storage devices containing special category or confidential data will undergo assessment to determine if the device should be destroyed, repaired, or discarded. Such devices will remain the property of the Foundation and only be removed from site with the permission of the information asset owner/Director of IT.

7.4 Working practices

The Foundation advocates a clear screen policy particularly when employees are absent from their normal desk and outside normal working hours. Employees should log out or lock their workstations when not in use. In addition, screens on which special category or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons. This applies to both fixed desktops and mobile devices/tablets.

7.5 Off-site removal of data

Removal off site of Foundation special category or confidential information, either in print or held on any type of computer storage medium, including tablets, phones or USB drives whether owned by the Foundation, or not, should be authorised by the relevant Senior Leader or Director and only in accordance with the Foundations Data Protection Policy.

Special category or confidential information must not be kept in a cloud storage service which is not approved by the Foundation.

7.6 Backup and recovery

The Director of IT and local academy information owners must ensure that tested backup and system recovery procedures are in place. Backup of the Foundation’s information assets and the ability to recover them are important priorities. In line with academy Business Continuity Plans, all

Headteachers/Principals and system managers must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles; especially where such files may replace files that are more recent.

7.7 Archiving

The archiving of information must take place with due consideration for legal, regulatory and business issues, with liaison as needed between IT staff, data protection leads and data owners, and in keeping with the Foundation's Record Management Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

7.8 Information lifecycle management

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity, and availability of such files. Day to day data storage must ensure that current information is readily available to authorised users. Any archives created must be accessible in the case of need.

7.9 Special category or confidential information

Special category or confidential data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured and in accordance with the Data Protection Policy. Special category or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

7.10 Use of electronic communication systems

The identity of online recipients, such as email addresses and fax numbers, should be checked carefully prior to dispatch, especially where the information content is special category or confidential. Information received electronically must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

Special category or confidential information should only be sent electronically (e.g. by email) to external recipients when it is encrypted or protected by a password.

7.11 Access to personal or individual data for systems management purposes

Some individuals may need access to personal data identifying individuals, or to data which belongs to others, in order to manage systems or to fix problems, for example IT support technicians. These individuals will be required to sign a data protection declaration before they are sanctioned to carry out these duties.

8 Mobile and Remote Computing

8.1 Authorisation

Those remotely accessing information systems, data or services containing special category or confidential information must be authorised to do so by an appropriate authority, usually their line manager.

8.2 Use of computing equipment off-site

Computers or other devices should only be used off-site for Foundation related activities if Foundation-approved security controls are in place. This provision applies to all equipment, irrespective of ownership. If special category or confidential information is being stored or accessed from off-site, only the member of staff concerned should use the equipment, unless the highest levels of security are in use and an approved access solution is used. No special category or confidential information is to be stored on any I.T. System that has not been approved by the Foundation.

8.3 Travelling

Portable computing or storage devices are vulnerable to theft, loss or unauthorised access when travelling. Foundation-approved mobile device management software must be installed and activated at all times. Devices must be provided with an appropriate form of access protection such as a password or encryption to prevent unauthorised access to their contents. Multi factor authentication must be in place across all academies. In addition, more recent means of authentication such as Touch-ID or Face ID are also acceptable forms of access protection.

Equipment and media should not be left unattended in public places and portable devices should be carried as hand luggage. To reduce the opportunities for unauthorised access, automatic shutdown features should be enabled, with laptops set to log out when the screen closes. Passwords or other similar security tokens for access to the Foundation's systems should never be stored on mobile devices or in their carrying cases. Screens on which special category or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.

Export and import controls apply when travelling to certain countries which restrict the use of encrypted devices. Advice should be taken from IT Support before any travel arrangements are made, as necessary.

Passwords should not be remembered on personal devices.

9 Outsourcing and Third-Party Access

9.1 External suppliers

All external suppliers who have access to Foundation I.T. Systems or data must work under the supervision of Foundation staff and in accordance with this Policy. A copy of the Policy will be made available to the supplier, if required.

Admin or elevated privileges will only be provided once a risk assessment and authorisation is granted.

9.2 Confidentiality declaration

The Foundation will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the Foundation will require external suppliers of services to sign a confidentiality declaration to protect its information assets. This will be the responsibility of the system owner, Director of IT and relevant academy data lead. Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of this Policy.

9.3 Service level agreements

Any facilities management, outsourcing or similar company with which the Foundation may do business must be able to demonstrate compliance with the Foundation's Information Security Policy and must enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

10 Operations

10.1 Building access control

Areas and offices where special category or confidential information is processed will be given an appropriate level of physical security and access control. Line managers will provide information on the potential security risks and the measures used to control them to staff with authorisation to enter such areas.

10.2 Operational procedures

System owners must ensure that the procedures for the operation and administration of the Foundation's business systems and activities are documented and that those procedures and documents are regularly reviewed and maintained. Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the Foundation.

10.3 Procedure for reporting concerns

System owners must ensure that procedures are established and widely communicated for the reporting to IT Support of security incidents and suspected security weaknesses in the Foundation’s I.T. Systems. They must also ensure that mechanisms are put in place to monitor and learn from those incidents. Where any IT security incident is felt to have an impact on data security, or there is a suspected Cyber attack, or if “something doesn’t look right”, this must be reported to the relevant data lead and IT Lead and logged on the GDPRiS platform, as well as the Cyber Reporting form, where a breach is deemed to have occurred (or a near miss). Faults and malfunctions must be logged and monitored, and timely corrective action taken.

10.4 Change management

Changes to operational procedures, systems or hardware must be controlled to ensure continuing compliance with the requirements of this Policy and must have management approval. Development and testing facilities for business-critical systems will be separated from operational facilities and the migration of software from development to operational status will be subject to formal change control procedures. Acceptance criteria for new information systems, upgrades and new versions will be established, and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place. Procedures will be established to control the development or implementation of all operational software, which must be approved by the Foundation’s Executive Group before introduction and a Data Privacy Impact Assessment must be completed and approved for any new system that will involve the processing of personal data. All systems developed for or within the Foundation must follow a formalised development process.

10.5 Risk assessment

The security risks to the information assets of all system development projects will be assessed by system owners and access to those assets will be controlled. Risk registers will be completed for major system development projects, with reference to associated information security risk.

11 User Management

11.1 User identification

System owners must ensure that procedures for the registration and deregistration of users and for managing access to all information systems are established to ensure that all users' access rights match their authorisations. These procedures must be implemented only by suitably trained and authorised staff. All users must have a unique identifier (user ID) for their personal and sole use for access to all the Foundation's information services, which should authenticate against the institutional directory where practicable and not shared with others. Users will be expected to sign separate documentation for the use of IT and any Trust owned equipment.

11.2 ID security

The user ID must not be used by anyone else and associated passwords must not be shared with any other person for any reason. Password management procedures must be put into place to assist both staff and students in complying with best practice guidelines.

11.3 Access control standards

System owners must establish appropriate access control standards for all information systems which minimise information security risks yet allow the Foundation's business activities to be carried out without undue hindrance. Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Procedures must be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the organisation. Users' access rights must be reviewed at regular intervals.

11.4 Starters, leavers and affiliates

The IT Leads must ensure that access to I.T. Systems is only available to employees during their period of employment. In particular, IT Leads must ensure that the system access of leavers is withdrawn as soon as employment is terminated. IT Leads must follow the Foundation's offboarding procedures. Line Managers are responsible for ensuring that any IT equipment is collected on departure from the organisation.

11.5 User training

All those who wish to access the Foundation's I.T. Systems must have successfully completed the training which is deemed appropriate for their role. Advice on what training is required is available from line managers or directly from the team who manages each system. This training should form part of onboarding procedures for all staff.

12 System Planning

12.1 Authorisation

New IT systems relating to teaching, research, or the administration of the Foundation, or enhancements to existing systems, must be authorised by the appropriate authority/SLT and added to the organisations primary MIS system. The business requirements of all authorised systems must specify appropriate security controls. The implementation of new or upgraded software or hardware must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

12.2 Risk assessment and management

System owners must ensure that the information assets associated with any proposed new or updated systems are identified, classified and recorded, and a risk assessment, including, where relevant, a data privacy impact assessment, is undertaken to identify the probability and impact of security failure. Equipment supporting business systems must be given adequate protection from unauthorised access, environmental hazards, and electrical power failures.

12.3 Access control

System owners must ensure that access controls for all I.T. Systems are set at appropriate levels in accordance with the value and classification of the information assets being protected. Access to operating system commands and application system functions must be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored and a record kept of any elevated privileges which have been authorised.

12.4 Testing

System owners, in consultation with IT Support Services, must ensure that prior to acceptance, all new or upgraded systems or hardware are tested to ensure compliance with this Policy and requirements for ongoing information security management.

13 IT Systems Management

13.1 Staffing

IT systems must be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with individual system owners. All systems management staff must have relevant training in I.T. security issues and know how to escalate potential security issues or identify breaches. All training should be logged on the relevant training platform/system.

13.2 Access control

System owners must ensure that access controls are maintained at appropriate levels for all I.T. Systems and that any changes of access permissions are authorised by the manager of the system or application. A record of access permissions granted must be maintained. Access to all I.T. Systems must use a secure login process and access may also be limited by time of day or by the location of the initiating terminal, or both.

System owners must ensure that all access to systems containing special category or confidential information is logged to identify potential misuse of systems or information. They must also ensure that password management procedures are put into place to ensure the implementation of security procedures and to assist users in complying with best practice guidelines.

Remote access to the network must be subject to robust authentication as well as appropriate levels of security using Multi factor authentication methods. Virtual Private Network, wireless, and other connections to the network are only permitted for authorised users.

Access to operating system commands must be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored.

13.3 Change management

System owners must ensure that the procurement or implementation of new or upgraded software is carefully planned and managed and that any development for or by the Foundation always follows a formalised development process with appropriate audit trails. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. Business requirements for new software or enhancement of existing software must specify the requirements for information security controls.

The implementation, use or modification of all software on the Foundation's business systems must be controlled. All software must be checked before implementation to protect against malicious code.

Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Support Services according to procedures laid down by them. All changes must be properly tested and authorised before moving to the live environment.

13.4 Network design

The Director of IT and IT Support Services must ensure that the Foundation data and telecoms network is designed and configured to deliver high performance and reliability to meet the Foundation’s needs whilst providing a high degree of access control and a range of privilege restrictions. Appropriately configured firewalls or other security devices must be used to protect the networks supporting the Foundation’s business systems.

13.5 Logging

System owners and IT Support Services must ensure that security event logs, operational audit logs and error logs are properly reviewed and managed by qualified staff. System clocks must be regularly synchronised between the Foundation’s various processing platforms.

14 Complaints

14.1 Complaints relating to the Foundation’s information security will be dealt with in accordance with the Foundation’s Complaints Policy.

14.2 Complaints relating to information data security should be made to our DPO who will decide whether it is appropriate for the complaint to be dealt with through the Foundation’s complaints procedure. Complaints which are not appropriate to be dealt with through the Foundation’s complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.

14.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 0303 123 1113.