Joseph Leckie Academy

Information Risk and Security Policy

Approved by JLA Trust Board:	09/2021
Last reviewed on:	10/2022
Next review due by:	10/2023

1. Introduction

1.1 Information is a vital asset to the Academy. Joseph Leckie Academy is committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision making
- to deliver quality services
- to comply with the law
- to meet the expectations and demands of our parents, students and Trustees
- to protect our reputation as a professional and trustworthy organisation.

1.2 The purpose of the Information Risk and Security Policy is to protect the Academy's information, manage information risk and reduce it to an acceptable level, while facilitating appropriate use of information in supporting customer demand and normal business activity for the Academy and other organisations that it works with. Information must be accompanied by appropriate levels of security at all times. 'Appropriate' is a degree of precaution and security proportionate to the potential risk, information category and impact of loss or accidental disclosure.

1.3 The Information Risk and Security Policy will ensure an appropriate level of:

Confidentiality. To ensure the confidentiality of information is achieved, access to Information is controlled and monitored accordingly based on the data category requirements, roles of individuals and processing conditions. Information is only accessible by those who require it and only disclosed lawfully where appropriate controls and assessments have been undertaken. Systems and information assets must also ensure that appropriate levels of security are in place at all times to protect the confidentiality of the data held within.

Integrity. Information must be accurate and up to date in accordance with the Data Protection Act and the General Data Protection Regulation (GDPR) 2016 alongside the rights of the individuals with regards to rectification and erasure. All information assets and systems must be assessed regularly to ensure compliance of these requirements.

Availability. Networks, systems and information assets should always be available when required to those with a justified right to access. This relates to business continuity and systems resilience, which ensure that data remains available and secured

Anyone handling personal, sensitive or confidential information must take personal responsibility and make considered judgments in terms of how it is handled whilst delivering Academy services. If in any doubt members of staff and or systems users should always seek advice from the Principal or the Data Protection Lead/Data Protection Officer.

1.4 The Information Risk and Security Policy will also make sure that:

- The Academy establishes a culture of care and security for information.
- Information is only obtained or shared when it is required.
- Information owned or processed by the school is protected against un-authorised access or disclosure.
- ICT equipment is protected from accidental or malicious damage.
- Information security risks are properly identified, assessed, recorded and managed.
- Information security incidents are reported and managed appropriately.

- Appropriate safeguards are implemented to reduce security risks.
- Legal and regulatory requirements are understood and met.
- Guidance and training with regards to information security is available and up to date.

1.5 Compliance with this policy will be achieved by:

- Ensuring that all individuals who work for or on behalf of the Academy are aware of and fully comply with the relevant legislation as described in this and other policies and procedures.
- Introducing a clear process for the recognition of data changes and the appropriate application and completing of data privacy impact and information security risk assessments.
- Ensuring that any assessments identify appropriate measures for risk identification and reduction.
- Introducing a consistent approach to security, ensuring that all individuals who work for or on behalf of the Academy fully understand their own responsibilities and have the appropriate tools to work with creating and maintaining a level of awareness of the need for information security as an integral part of day to day business.
- Reporting and investigating all breaches of information security, actual or suspected.

2. Scope

2.1 This policy applies to all individuals working for or on behalf of the Academy who use or have access to Academy information assets, computer equipment or other ICT facilities.

2.2 The policy applies throughout the lifecycle of the information from creation through to storage, use and transfer to retention and disposal. It applies to all information including, but not limited to:

- Information stored electronically on databases or applications both on site or in the cloud.
- Information stored on computers, PDAs, mobile phones, printers, or removable media such as hard disks, CD, memory sticks, tapes and other similar media.
- Information transmitted on networks or via the internet and or social media platforms.
- Information sent by email, fax or other communications method.
- All paper records including information sent out by post.
- Microfiche, visual and photographic materials including slides and CCTV.
- Spoken, including face-to-face, voicemail and recorded conversation.

3. The Policy

3.1 Information Assets & Risk Management. All Academy information assets must be risk assessed and measures put in place to ensure each asset/system is secured to an appropriate level based on the measure of risk associated with it. This process will involve identifying threats and vulnerabilities (severity of impact and the likelihood of occurrence) at an individual asset level and the analysis and assessment of risks in order to make the best use of resources.

Information security risks must be recorded within a baseline risk register and action plans put in place to effectively manage those risks. The risk register and all associated actions must be reviewed at regular intervals. Any implemented information security arrangements shall also be regularly reviewed.

Overall responsibility for information security risk management will rest with the Principal but day to day management will rest with the Data Protection Lead.

4. Information Asset Security & Confidentiality

4.1 Information risk and security management controls and procedures for all information assets will conform to the International Standard for Information Security ISO27001:2013 and the associated code of practice ISO27002:2013.

4.2 The security of all information assets must be considered at all stages of the asset lifecycle. The risks associated with handling, storing and sending information must be identified and mitigated, giving due regard to the Common Law Duty of Confidentiality. Processes for handling information assets must give regard to relevant statutory and regulatory requirements.

4.3 The Academy's ICT systems, processes and infrastructure will be designed and maintained to ensure that:

- Appropriate measures are in place to protect the Academy's information and systems from damage or loss due to malicious software such as viruses and or cyber-attacks.
- Information is available when required i.e. by ensuring that information and information systems are available to authorised users at point of need and appropriate business continuity and disaster recovery processes are in place and audited regularly for functionality.
- Robust password and access control regimes are in place and maintained.
- Managers are aware of their responsibilities with regards to authorizing and monitoring systems access.

4.4 Where equipment and devices are no longer required the IT Support will ensure that devices are appropriately cleansed for reissue or destroyed in accordance with the internal processes requirements and national standards.

4.5 Equipment will not be reallocated or reissued without appropriate data cleansing in line with the government standards such as IS5 (information security standard).

4.6 External or third party systems: In addition to the above, line managers must also ensure that they follow any password and or security controls applied by third parties and that appropriate agreements or controls are in place to ensure secure access to information being shared with the Academy and utilised within the network.

5. Access Controls

5.1 Individuals given access to Academy information assets should only access systems that they have authority for. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems without authority to do so. Un-authorised access to information systems or information contained within a system will also be recognized as serious breach of confidentiality under the data protection regulations.

5.2 **Systems access:** Formal procedures are used to control access to IT systems. Most systems employ role based access controls (RBAC) where access is granted based on a user's role and justified requirements.

Least privilege basis access (users are only granted access to parts of the network, systems or applications that their job role requires). In some cases, this may result in view only access being granted unless otherwise justified and authorised.

For access to be granted, an authorised manager must contact ICT by email or using the work request process stating the access level required.

5.3 **Leaving or moving:** When individuals leave the Academy or move to another team it is their manager's responsibility to ensure that access is amended or accounts are disabled/deactivated. User access rights will be reviewed, monitored and audited on a regular basis (at least annually).

5.4 **Password Management:** Passwords must be changed when prompted and strong passwords should be used e.g. 15 characters including at least one capital letter one lower case letter and a special character (!£$%&*). Passwords must not be written down or shared with anyone else. A short memorable phrase can be used to aid memory.

5.5 **Third Party Systems Access:** Third parties requiring access to Academy systems for maintenance and support must sign a 3rd party access agreement before access is granted or be supervised on site by a member of IT Support.

6. Equipment Security

6.1 To mitigate the risks of loss, damage, theft or compromise of equipment and to protect equipment from environmental threats and hazards, and opportunities for un-authorised access:

- Equipment in the Academy's data centre's will be protected from disruptions caused by failures in supporting services e.g. Power failure, air conditioning failure
- All equipment will be correctly maintained to ensure correct (specified) operation and uptime
- Security settings and software must not be altered without prior permission from IT Support.
- Regular patches and software updates are applied in line with the IT patch process. These ensure the Academy is operating its network and systems using the latest safeguards and security controls.

7. Mobile Working

7.1 Mobile working is permitted and is subject to prior approval and the following precautions must be adhered to:

- Always ensure devices or information are protected appropriately in accordance with this Policy and Framework.
- Always work in an appropriate environment that ensures the confidentiality and security of any information being accessed.
- Never install or use unapproved software or memory devices.
- Never leave mobile devices in open areas, unattended vehicles or unsecure locations.
- Never provide access to un-authorised or unapproved persons.
- Never remove the security or access controls applied to school devices
- Never store passwords with devices.
- Ensure devices are charged regularly and logged on and connected to the school network at least once a month for a period of at least two hours so that appropriate patches and security updates can be applied.

- Report any loss or theft of mobile devices immediately to your direct manager and to IT Support.

8. Screen Timeout Procedures

8.1 Inactive computers are set to time out after a pre-set period of inactivity. The time-out facility will clear and lock the screen.

Users must lock their computers, if leaving them unattended using the Ctrl/Alt/Delete or Windows and L keys. (see Fig. 3)

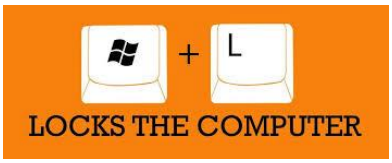

Fig 3: Quick Lock Option

9. Use of Removable Media

9.1 It is the Academy's policy to prohibit the use of all un-authorised removable media devices including USB sticks for the storage of personal data. The use of removable media devices will only be approved if a valid business case for its use is provided. Please see the Portable Device and Storage Policy.

10. Information Classification

10.1 All information within the Academy will be identified and classified by the criteria set out in the Academy's Protective Marking Procedure.

10.2 This will ensure that information is given the appropriate level of protection when it is processed. Classification may change at any point in the information lifecycle e.g. a document may have a different classification when it is created to when it is approved and available for circulation. Information that is not classified will assume the lowest classification of 'Not Protectively Marked'.

11. Posting, emailing, faxing and printing information

11.1 When sending information either inside or outside the Academy the appropriate method of transmission must be used according to the confidentiality or sensitivity of the information and the classification it has been given.

11.2 The risk of harm or distress that could be caused to the individual(s) that the information relates to if it were lost or sent to the wrong recipient should be considered when making the decision on the most appropriate method of transmission.

11.3 It is important that only the minimum amount of information required is sent, by whichever method is chosen.

11.4 When sending information by email the sender must:

- Carefully check the recipient's email address before pressing send – this is particularly important where the recipient fields are automatically populated by the system.

- Take care when using the 'reply all' function – are all the recipients known and do they all need to receive the information being sent.
- Ensure that personal, sensitive or confidential information is not included in the subject field or body of an email. If sensitive information has to be sent via unsecure email, password protected attachments must be used. A different transfer method must also be used to communicate the password e.g. Telephone call, separate email or text
- Secure email must always be used for sending personal, sensitive or confidential information, if it is available.
- The use of personal or home email addresses for Academy business is strictly prohibited.
- When using email to communicate with other public sector network partners such as health, police or local authorities always use the approved secure email system (e.g. GCSX, GSI, CJSM, etc.) especially when sharing personal, confidential, sensitive information.

11.5 When sending information by post the sender must:

- Ensure that the name and address details are correct – window envelopes should be used whenever possible to avoid errors in transcribing details.
- Ensure that only the relevant information is in the envelope i.e. The information is adequate, relevant and not excessive.
- That envelopes containing personal, sensitive or confidential information are marked 'private and confidential – addressee only'.
- That a return address is added/printed on the back of the envelope.

11.6 When sending information by fax the sender must:

- Telephone ahead to advise the fax is being sent and ask for confirmation of receipt.
- Check the fax number is correct and dial carefully.
- Attach a cover sheet to the fax indicating who it is for, the fax number it has been sent to, the contact details of the sender, the date and number of pages (including the cover sheet) in the document.
- If the information is particularly sensitive (and it cannot be sent by a more secure method) consider sending a test fax to ensure it reaches the correct recipient.

11.7 When printing or photocopying information always ensure that:

- Secure printers are used wherever possible.
- If unsecure printers are to be used, only ever print the minimum required.
- Prints are always collected immediately.
- Check the document to ensure you have collected every print out.
- Ensure the printer has enough paper to complete your print.
- Ensure multiple documents are separated accordingly to avoid misfiling.

12. Physical and Environmental Security

12.1 Depending upon the function and the nature of use, offices where information is held will be equipped with appropriate security controls e.g. CCTV, entry controls etc. Public areas, deliveries etc. will be isolated from information processing areas.

12.2 Offices that deal with personal and/or sensitive information will have entry controls and lockable storage facilities.

12.3 ID cards, keys and other entry devices must be returned when access is no longer required.

12.4 All visitors must have official identification passes issued by the Academy. If temporary access to systems is given, a third party access agreement must be signed and access must be disabled when the visitor leaves. Visitors should not be afforded opportunity to view computer screens or printed documents without authorisation.

12.5 Strangers in office areas without an ID badge should be challenged or reported. Tailgating is not permitted.

12.6 Anyone handling personal, sensitive or confidential information is required to clear paperwork from their working area when leaving it for any length of time and always at the end of each working day Paperwork should be locked away securely.

13. Equipment and Data Disposal

13.1 If a device has ever been used to process Academy data, action must be taken to ensure data is irrevocably removed as part of the disposal process. All equipment that is past its useful life must be returned to IT Support for disposal. The Academy has a documented procedure for the disposal of equipment.

14. Intellectual Property Rights

14.1 All users must ensure that only licensed software issued or approved by IT Support/Principal is installed on Academy equipment. The loading and use of unlicensed software on Academy computing equipment is not permitted. All users must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate license to prove the software was legally acquired. The school monitors the installation and use of software. Any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the Academy's disciplinary procedures.

15. Systems development, planning and procurement

15.1 All system developments must comply with the Academy's ICT Strategy. Security and risk management issues must be considered and documented during the requirements and procurement phases of all procurements and developments which affect data relating to Academy activity, Academy customers, partners, employees or suppliers.

15.2 Privacy by design is an approach that promotes privacy and data protection compliance from the start. The General Data Protection Regulations (GDPR) has introduced a legal requirement for Data Protection Impact Assessments and privacy by design in certain circumstances.

15.3 The Academy will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout the project lifecycle. Projects would include, but not limited to:

- A new IT system
- A new data sharing initiative
- A proposal to identify people in a particular group or demographic

- Using existing data for a new or more intrusive purpose
- Introduction of a new CCTV system or the application of new technology to an existing system

15.4 IT systems are checked both internally and by external accredited suppliers on a regular basis for security and technical compliance with relevant security implementation standards including:

- Public Services Network connection
- Payment Card Industry Data Security Standard (PCI/DSS)

16. Data Changes

16.1 In order to gain assurance that information is handled securely, legally and in line with any legislation or Information Governance requirements the inclusion of Information Governance and Privacy must be taken into account at the beginning of new projects or processes that affect the way in which information is handled.

16.2 Staff must not purchase new systems, mobile technology devices, and external services or implement process changes that involve the use, creation, storage and or sharing of personal, sensitive or confidential data without first obtaining approval from the Principal.

16.3 Depending on the information you provide the Principal may ask you to complete:

- Information Security Assessment (ISA)
- Data Protection Impact Assessment (DPIA)
- Site or Premises Assessment form

16.4 Where data processing is involved it may also be necessary to ensure that IG or DPA (Data Protection Act) clauses are included in contracts and or sharing, processing agreements.

16.5 The Principal and the Data Protection Lead undertake assessments to provide assurance that all personal/confidential information is secure in accordance with the GDPR, DPA and DSP Toolkit requirements.

16.6 Next Steps:

Please make sure you consider the following points before ordering, buying or making changes to the way in which data is held or collected within the Academy:

- Is this something that includes the storage or use of student, parent/carer or staff information?
- Are you changing a process, contract or Service Level Agreement (SLA) that involves student, parent/carer or staff information?
- Are you purchasing something that will be used for the processing of student, parent/carer or staff information?
- Are you purchasing something that will be used for the processing of business information?
- Is a third party organisation going to be processing any personal or special category (sensitive) data on your behalf?

16.7 If you have answered yes to any of the above questions, then you will need to speak to the Data Protection Lead and obtain approval from the Principal.

17. Cyber Security

17.1 Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the school. In the event of a successful attack this may also result in loss of data, potential for monetary penalties and additional replacement systems or equipment costs to rectify any data losses or disclosures and or systems functionality.

17.2 Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

17.3 Foreign states, criminals, hackers, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- Financial gain.
- Attracting publicity for a political cause.
- Controlling computer infrastructure to support other nefarious activity.
- Disrupting or destroying computer infrastructure stealing sensitive information to gain economic, diplomatic or military advantage.

Academy employees can also be targets for criminal activity.

17.4 As with most schools, Joseph Leckie Academy relies heavily on access to the internet and to information held in its systems. There are several IT systems/services that have an internet presence e.g. the Academy website or the ability to work from home and there are several different ways gain access to information e.g. Wi-Fi, physical networking, mobile phones, tablets etc. All can present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the Academy employs a range of tools and good practice to minimise the risk to its information and systems.

17.5 The Academy has clear procedures and guidance on Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Removable Media
- Sharing and disclosing information

17.6 The Academy implements security controls and good practice to enable it to achieve compliance with Public Services Network (PSN), Payment Card Industry Data Security Standards (PCI DSS) and the NHS DSP Toolkit. All of these require the council to ensure that systems are security patched and that the school has regular penetration tests of its network/systems that are performed by a third party.

18. Information Sharing

18.1 This policy supports effective and appropriate information sharing across the Academy and with partner organisations as part of overall service improvement. Sharing of information with partners is subject to appropriate information sharing/processing agreements and the requirements of the Data Protection Act 2018 and the GDPR 2016. Information sharing with other

external organisations should also be supported by a purpose specific information sharing/processing agreement. All agreements should be made in consultation with the Principal and Board of Trustees.

19. Breach Management

19.1 The Academy's Procedure for Reporting and Managing Data Breaches must be followed wherever there is any un-authorised or unlawful disclosure, loss, damage or destruction to personal or confidential information. Anyone granted access to Academy information is responsible for reporting any actual or suspected breach as soon as it is discovered and must be aware of the procedure and the reporting requirements.

20. Business Continuity Planning

20.1 All systems and information assets will have threats and vulnerabilities assessed by system owners to determine how critical they are to the Academy. The Academy's business continuity planning process will include consideration of information security gained from the information asset and risk register.

21. Contracts

21.1 If contracts involve exchange of personal or sensitive data a DPIA must be completed and approved and if services are hosted elsewhere a Technical Assessment must also be completed and approved as part of the procurement process.

21.2 Prior to award of a contract a Data Processor Agreement or Contract must be implemented and signed by any 3rd party handling personal information on behalf of the school providing assurance that they comply with the Data Protection Act 2018 and the GDPR 2016 requirements if processing relate to personal or special category (sensitive) data.

21.3 All new contractual arrangements with suppliers of goods or services to the Academy will contain confirmation that the suppliers comply with all appropriate information security policies and procedures in accordance with the guidance on contractual clauses as provided by the Information Commissioners Office.

22. Contracts of Employment

22.1 Information security expectations of employees shall be included within job descriptions and person specifications where appropriate.

22.2 Pre-employment checks will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements this may involve requirements for BPSS/DBS checks.

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

22.4 Annual Information Governance (Data Protection) training is a national legal requirement that the Academy must comply with.

23. Personal Use

23.1 Personal use of Academy ICT equipment is permitted providing that it is in line with the

provisions of the Acceptable Use Policy, the Staff Code of Conduct and other procedures relating to the use of Academy devices.

24. Social Networking and Media Platforms

24.1 In order for the Academy to improve its accessibility and visibility on social media sources, a policy and supporting guidance is required to ensure that any regulatory or professional, legal requirements are fully understood and met.

24.2 This policy provides staff with clear guidelines on:

- Acceptable use of social media linked to their employment
- Acceptable use of social media for the purpose of academy business
- Being mindful of any content they share on such platforms
- Maintaining appropriate standards of confidentiality
- Maintaining and protecting professional boundaries with service users

24.3 All staff are expected to follow the staff code of conduct, employment contracts and Academy policies at all times.

24.4 Academy employees will not use or maintain a social networking site that contains:

- Personal identifiable information of Academy employees, students or parents/carers.
- Personal identifiable information of other Academy employees in relation to their employment, including judgements of their performance and character.
- Photographs of other Academy employees, students or parents taken for the purpose of social networking without full and explicit consent in line with the Consent to use Personal Data guidance.
- Statements that bring the Academy, its services, its staff or contractors into disrepute.
- Academy confidential or business information must not be loaded onto a private or business social networking site without the appropriate senior managerial sign off and without compliance of the Academy publication scheme.
- Employees must examine carefully any email or message coming from social networking sites or contacts, as these may be unreliable, contain malicious codes, be spoofed to look authentic, or may be a phishing email.
- Employees should not conduct themselves in ways that are detrimental to the Academy.
- Employees should take care not to allow their interaction on these websites or platforms to damage working relationships between members of staff, students or parents/carers.

24.5 Information security is implemented to protect and provide adequate security levels for information containing personal, sensitive and or confidential information relating to an individual or the business. It is vital that Social Networking forms part of this policy and supports this policy in order to protect the organisation, its staff and ensure that at all times the Academy is fully compliant with any Data Protect
ion Regulations or legal requirements.

24.6 There are 3 main elements for the use of social media sites within Academy services or functions:

- **Permission**
  - Teachers and managers must gain approval from the Principal for the creation and or use of social media sites and outlets.
  - Un-authorised use of social media to promote the school is a breach of these policies and will be managed in line with Academy disciplinary proceedings and potential dismissal or suspension.
- **Integrity**
  - Ensuring that information is accurate and can be modified by authorised persons only
  - Staff must follow policies for the use of a social network, site or any external web application.
- **Accountability**
  - The senior leadership team are responsible for ensuring that those using social media to support services as part of a business function, comply at all times with the required and appropriate policies, procedures and codes.

24.7 This will ensure that the Academy complies with legislation and standards relating to the use of social media, including the Computer Misuse Act, ISO27001 (International Standards for Information Security) and the Confidentiality Code of Practice: Information Security Management.

25. Further Information and Associated Policies

25.1 For further information about Information Governance please visit the ICO website www.ico.org.uk

25.2 This policy should be read alongside:

- Information Governance Strategy
- CCTV Policy
- Data Protection Policy
- Confidentiality Policy
- Freedom of Information Policy
- Information Rights Policy
- Records Management Policy and Schedule
- Incident Management Policy
- Subject Access Request Policy
- Consent to Use Personal Data Guidance
- Impact Levels and Protective Marking Guidance