William Austin Junior School

Information Security Policy

1 Introduction and scope

1.1 This document provides a précis of key school policies that help ensure the safety and security of sensitive organisational records; including those relating to our citizens and employees.

1.2 Each policy relates to a discrete area of information stewardship, but taken together they provide a guide to best practice as well as ensuring compliance with legal and regulatory standards that include:

- The Data Protection Act
- Minimum mandatory standards for Information Handling in Local Government
- GCSx Code of Connection
- Payment Card Industry Data Security Standards

1.3 The polices apply to governors, staff of our school, contractual third parties who have access to, or custody of pupil, staff and employee information

1.4 Further reading

1.4.1 Although this document provides a summary of key policy requirements, we must still read the policies themselves as they form part of our terms and conditions of employment.

1.4.2 All the policies, plus FAQs and other supporting information are available [where are policies available].

2 Information Security – Policy Framework

2.1 Key Messages

2.1.1 Ownership of information and systems

- All implementations (systems, facilities and services) will be assigned an Asset Owner, responsible for managing associated security, compliance and risks.
- All information will be assigned an Asset Owner, responsible for ensuring that information is managed in accordance with school policy
- Ownership of an asset should reflect the likely impact of any potential breach of confidentiality, integrity or availability of that asset or information associated with it
- Guidance on determining the impact of any loss of security can be found in the Information Classification and Handling policy
- Responsibilities of the Asset Owner and other users of school information are defined in within these policies

2.1.2 Risk management

- An asset owner will be assigned to all information assets
- All ICT projects will include a risk assessment component
- All ICT project risks will be assigned a risk owner responsible for producing a risk treatment plan to address the risk
- Governors will agree what is an acceptable benchmark for risks to ICT assets on a 6 monthly basis

- Where an information asset is observed to exceed this benchmark a risk treatment plan must be developed by the information asset owner, liaising with our Data controller as required
- All risks, in excess of the benchmark will be recorded in our school Risk log
- Governors or a delegate nominated by governors will act as arbiter in disputes over how identified information security risks should be remedied

2.1.3 3rd party service provision

- The framework and policies recognise that where information or systems used for provision of school services is hosted by a 3rd party, the need for continued compliance is retained and that controls agreed with the 3rd party will be at least equivalent to those operated by us.

3 HR Information Security Standards

3.1 We all need to be aware of and understand, these policies:

3.1.1 Anyone who needs regular access to the Government Connect Secure Extranet (GCSx) or who accesses protectively marked data (PROTECT, RESTRICTED, CONFIDENTIAL) must undergo baseline vetting (BPSS)

3.1.2 Once vetted, we must receive appropriate information security awareness training plus regular updates in related statute and organisational policies and procedures as relevant for our role

3.1.3 Once trained, we must sign a GCSx Acceptable use policy / Commitment statement

3.1.4 This needs to all be a formal auditable process, as we will be audited by Government security auditors regularly against this and the policies

4 Access Control Policy

4.1 General access

4.1.1 Any requirement for access to school Information Systems and data must be determined by a school business requirement.

4.1.2 Access to systems and data will be granted on the basis of 'least privilege' i.e. access granted should be sufficient to let us undertake our designated role, but no more.

4.1.3 Access to program code will be restricted to Information Management (IM) development staff and others as defined by the IM Systems Services Manager.

4.1.4 Enrolment of all users of our private network will be conducted by the Information Management Systems Administrator on receipt of a properly authorised request.

4.1.5 Enrolment of users onto specific applications is conducted by the designated Application Administrator on receipt of a properly authorised request from the System Owner or their delegate.

4.1.6 Changes in levels of access may only be conducted by designated Systems or applications administrator on receipt of a properly authorised instruction

4.1.7 Access to our school's private network will be reviewed every 6-12 months by [SLT] and System Owner or their delegates.

4.1.8 All network users will be assigned an individual user account. This account will be unique and personal to that user and may not be shared with others. The use of a secondary account or a generic account will only be permitted on (i) Submission and approval of a valid business case by the Headteacher or their delegate and (ii) Where compensating controls exist to minimise any risk associated with this activity.

4.1.9 Password complexity for our school's private network will comply with the legal and statute and mandatory requirements currently:

- Minimum 8 characters
- Password expires every 60 days
- Password must include a capital letter and a number
- No reuse of same password within 20 cycles

Similar levels of complexity are recommended for applications but are not mandated

4.1.10 Access to systems will be logged where this is necessary to ensure compliance with the legal and statute and mandatory requirements

4.1.11 Access to other Information systems or data will be logged at the discretion of the Head of Information systems or where relevant the designated owner of a system or data.

4.1.12 Employee access rights will be determined and a periodic review of individual access requirements, including systems access, access hours and remote access carried out. The review will be conducted periodically by IT Manager the outcomes recorded and necessary changes implemented.

4.1.13 Access to information systems and data shall be removed in a timely manner upon suspension or termination of employment, contract or agreement.

4.2 Remote Access

4.2.1 Remote access to the School's private network will comply with the Remote and mobile working policy

5 Desk and Workspace Security Policy

5.1 General

5.1.1 The following items must not be left unattended

- Sensitive Information including information classified as PROTECT, RESTRICTED or CONFIDENTIAL
- School Photo ID passes
- Keys to school property
- School owned cameras, iPads/tablets, mobile phones
- School owned memory sticks, CDs, DVDs, external hard drives, laptops or other removable media

5.1.2 Opportunities for loss, opportunist or premeditated theft of Information and equipment should be minimised

5.1.3 Any loss or theft should be reported at the earliest possible opportunity

5.2 IT equipment

5.2.1 Only school computers/laptops may connect directly to our private network

5.2.2 Only school owned phones, PDA's, cameras, memory sticks and other peripherals may be connected to school computers or our school's private network. See also Removable Media policy

5.2.3 Computer screens must be locked if they are likely to be unattended for more than a few minutes

5.2.4 School computers will have locking screensavers that will activate automatically if the device is not used for a specified time. Any exception to this will require both a business case and evidence of other mitigating controls and must be approved by the Headteacher or their delegate

5.2.5 School provided computers, computer peripheral and telecommunications equipment must be provided for inspection on request

5.2.6 Both work related and personal information may be viewed during such inspections and if relevant produced as evidence in any investigation or hearing relating to an alleged breach of School standards.

5.3 Telephones

5.3.1 Information that has been classified as RESTRICTED may not be disclosed in telephone conversations

6 Removable Media Policy

6.1 No removable media device may connect to a school computer unless there is a clear business reason for doing so

6.2 Use of any removable media devices that have not been purchased through IM procurement should be seen as highly exceptional

6.3 Where highly exceptional circumstances exists the 'Virus scanning removable media' procedure must be followed

6.4 All removable media devices must be virus scanned prior to use

6.5 All PROTECT or RESTRICTED data stored on removable media devices must be stored on a device that meets Government Connect minimum standards

6.6 Where CONFIDENTIAL data must be stored or removable media advice must be sought

6.7 Damaged or faulty removable media devices must not be used and any fault reported

6.8 Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage

6.9 Theft, loss or misuse of any removable media device must be reported

6.10 Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.

6.11 Line Managers must retrieve removable media devices from leavers etc.

7 Information Security Incident reporting

7.1 We should report any Information Security events, weaknesses and incidents by contacting the [IT Manager/Service Desk]

7.2 Anonymous reporting options are available if required; please see our school Whistle-blowing policy for more information

7.3 Out of normal office hours reporting methods are available via the Headteacher at admin@williamaustin.juniorluton.co.uk

7.4 We will assess and prioritise all security events and weaknesses and investigate all security incidents

7.5 Response to security incidents will be appropriate to the impact/potential impact of the incident

7.6 Incidents with a significant impact or potential impact may be escalated to either 'major Incidents' or 'disasters'

7.7 Where a major incident is declared the Information Management (IM) Major incident management procedure will be followed

7.8 Where a disaster is declared the School's Business Continuity policy and procedures will be followed

7.9 We will undertake regular reviews and trend analysis of Information Security weaknesses, events and incidents and report findings to SMT and the Governors

7.10 Where any element of this policy requires clarification advice should be requested by e-mail to the Business Manager in the first instance

7.11 Security events that are not information IT related should be reported to SMT in the first instance.

8 Software policy

8.1 All software must be purchased through the IT Manager

8.2 All software must have a valid license, registered to our school

8.3 Software may only be installed by specified, competent individuals as designated by the IT Manager/Precedence

8.4 On completion of installation all disks/copies of the software must be lodged within the software library managed by the IT Manager/IT Technician

8.5 Our school retains the liability for legal compliance and any associated penalties where installed software was previously purchased by directly by our school rather than through Information Management

8.6 Under no circumstances should personally owned software be installed

8.7 Under no circumstance should unsolicited software (this definition includes games and wallpapers etc.) be installed; this introduces a serious risk of computer virus infection

8.8 Copying of software is prohibited except where permitted by the terms of use for that product

8.9 Where software is developed on behalf of our school, ownership of the Intellectual property must be agreed and defined within the contract for the work

8.10 Where support for software is provided by a 3rd party a contract or this work must exist

8.11 Changes to software must be agreed with the asset owner and where implemented by Information Management should be in line with ITIL standards

8.12 Where changes are to be made by a 3rd party equivalent change control standards should be enforced by contract terms and conditions

9 Remote and mobile working policy

9.1 All ICT equipment (including portable computing devices) supplied to users is the property of our school and must be returned by the user either on the request of our school or when the user is no longer working on behalf of our school.

9.2 Access to ICT equipment must be provided on request to employees or school's Information Management (IM) service, for the purposes of installation, maintenance, monitoring or decommissioning

9.3 Any IT equipment supplied to or and installed within our school must be purchased via Information Management. An exceptions process will exist for equipment required as a reasonable adjustment under the Disability Discrimination Act.

9.4 Under no circumstances shall non-school owned equipment be used to access, e-mail or systems, files or folders that contain RESTRICTED information

9.5 Under no circumstances shall access to e-mail or systems, files or folders that contain RESTRICTED information be provided to any user or any device located outside of the United Kingdom

9.6 CONFIDENTIAL Information may not be remotely accessed

9.7 School provided ICT equipment must be provided for inspection on request

9.8 Both work related and personal information may be viewed during such inspections and if relevant produced as evidence in any investigation or hearing relating to an alleged breach of school standards

10 Information and Classification and handling Policy

10.1 As of right now…

10.1.1 Information sent via [Egress] must be labelled appropriately (Unclassified, PROTECT, RESTRICTED, CONFIDENTIAL)

10.1.2 If data is already protectively marked by e.g. DWP it should be handled in accordance with its classification

10.1.3 School data that isn't protectively marked only needs to be classified if it's being sent via Egress.

10.1.4 Egress is available to connect the sender and receiver of the protectively marked information, this must be used

10.1.5 Sending protectively marked information to any external organisation is prohibited, unless via Egress.

10.1.6 Emails sent between school email addresses never actually leave our school private network and are therefore secure.

10.2 Coming in the near future

10.2.1 We will draw up and maintain inventories of all important information assets

10.2.2 These assets will be assigned an owner within the business

10.2.3 All information assets, where appropriate, will be assessed, classified and labelled by the owner Once an asset is classified it must be handled appropriately

11 Communications and Operations Management Policy

11.1 Change control within IM

11.1.1 Documented procedures must exist for data handling and management e.g. ISO9001

11.1.2 Changes to IT infrastructure and systems need to be documented and done in a controlled manner e.g. ITIL

11.1.3 Separate environments need to exist for development, testing and live (operational) systems

11.1.4 Capacity planning must be undertaken for key systems and infrastructure

11.2 Change control requirements that will impact outside IM

11.2.1 The Asset Owner must be assigned for all existing and planned systems

11.2.2 The Asset Owner must ensure there is a process for finding out about software vulnerabilities and available patches

11.2.3 The criteria for what is an 'acceptable system' or product must be clearly defined and agreed with the Asset Owner at an early stage of the project, upgrade or installation

11.2.4 If solution delivery is undertaken by a third party on behalf of the School the Asset Owner must ensure that equivalent Systems acceptance processes are agreed and applied

11.3 Public facing systems

11.3.1 Public facing systems i.e. school systems used by the public or available from the internet must be security tested prior to going live.

11.3.2 If these systems are upgraded they must again be hardened, patched and security tested before going live

11.3.3 All security tests will be arranged through Information Management

11.3.4 It is the responsibility of the Asset Owner to ensure that when System delivery is undertaken by a third party on behalf of the School, equivalent Security testing processes are agreed and applied

11.4 Protection against malicious and mobile Code

11.4.1 Effective and up-to-date anti-virus software will be run on all servers and PCs

11.4.2 We must check regularly to ensure that Anti-virus software on computers are current and fully functional.

11.4.3 We must scan all removable media for viruses as described in the 'removable media policy.

11.4.4 Where a virus or malware is detected the event will be reported to Precedence at the earliest practical opportunity

11.5 Backups and disaster recovery

11.5.1 Regular backups of essential business information must be taken and an appropriate backup cycle must be used and fully documented.

11.5.2 Back-up media will be stored securely off-site

11.5.3 Local service continuity plans will be maintained and tested by our school as detailed in the 'Business Continuity Policy'

11.6 Disposal of storage media

11.6.1 Storage media that is obsolete or no longer required must be destroyed in a secure and environmentally friendly manner. This must include thorough removal of all data from the storage media to avoid the potential of data leakage.

11.7 School information held by a third party

11.7.1 It is the responsibility of the Asset Owner to ensure that where information is stored by a third party on behalf of the school, equivalent back-up, storage transit, recovery and disposal regimes are agreed and applied.

11.8 Monitoring

11.8.1 Audit logs of key system events e.g. log on, log off and access to sensitive information will be recorded and reported upon

11.8.2 A minimum of 6 months of logs will be held

11.9 Annual IT health check

11.9.1 An annual health check of all school IT infrastructure systems and facilities must be undertaken by Information Management every 12 months.

All users must understand and adopt this policy and ensure that we act within the law when working on school systems and information. In particular users must consider the implications of the legislation listed below.

12 Legal Responsibilities Policy

12.1 General

12.1.1 Our school must ensure that all users are aware and of their key legal obligations in relation to the ICT equipment, systems and information accessed, used and stored

12.1.2 We will provide advice and where appropriate will provide training in legal matters relevant to Information security.

12.1.3 We must ensure we aware of and adhere to these key legal obligations

12.2 Relevant legislation

These may include:

- Copyright Designs and Patents Act (1988)
- Computer Misuse Act (1998)
- Data Protection Act (1998)
- Freedom of Information Act (2000)
- The Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000) aka RIPA
- The Electronic Communications Act (2000)
- Environmental Information regulations (2004)
- Reuse of Public Sector Information Regulations (2005) **
- Criminal Justice and immigration act (2008)

- Statutory Instrument 2003 No.2426 'The Privacy and Electronic Communications (EC Directive) Regulations (2003)

12.3 Relevant mandatory requirements

These may include:

- Government Connect Code of Connection (Co-Co)
- Payment Card Industry Data Security standard (PCI DSS)

13 IT Infrastructure Security Policy

13.1 Physical security

13.1.1 Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted.

13.1.2 The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there.

13.1.3 Particular attention will be paid to data centres and telecommunications equipment rooms.

13.2 Baseline secure areas

13.2.1 All buildings and rooms within the school are as a minimum deemed baseline secure areas at times when they are not open to the public.

- Within baseline secure areas:
- We must display their PhotoID and must challenge anyone not displaying appropriate school passes (PhotoID)
- We must ensure that doors and windows are properly secured
- Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

13.3 Enhanced secure areas

13.3.1 The designation of an enhanced secure area will take into account the impact of loss of confidentiality, integrity of availability to data within that area plus other risks including theft or personal injury to persons in that area.

Within enhanced secure areas, security is as per baseline secure areas plus:

- Visitors are required to sign in and out with arrival and departure times and are required to wear an identification badge.
- If the area contains key ICT infrastructure components a member of the school's Information Management team must monitor all visitors.
- Keys to any enhanced secure areas housing key ICT infrastructure components will be held securely by Information Management

13.4 Responding to incidents for any area

13.4.1 Contacting emergency services or any locally based security personnel will usually precede any other action

13.4.2 We may contact emergency services or on site security personnel without need for further authorisation

13.4.3 We must not put themselves, our colleagues or customers at risk of physical harm or injury

13.5 Incidents in baseline or enhanced secure area

13.5.1 The incident must additionally be reported to SMT who must in turn advise the emergency services

13.5.2 All employees – Where a security breach involves a threat to Information Security, the incident must also be reported to the Data Controller See 'Information Security Incident Management policy.

13.6 Paper based information

13.6.1 Where a document is protectively marked, appropriate information security controls to protect it must be put in place. These may include:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

13.7 ICT equipment

13.7.1 Computer equipment must be sited to minimise risks from environmental hazards, from theft or from unauthorised people being able to look at our screens

13.7.2 Data should always be stored on the network file servers in preference to our computer hard drive or removable media

13.7.3 Servers must not reside outside designated data centres, which in turn will be deemed 'enhanced secure areas' and protected accordingly

13.7.4 All ICT equipment must be security marked and have a unique asset number allocated to it that cross references to inventory

13.8 Equipment maintenance

13.8.1 ICT Equipment must be maintained in accordance with the manufacturer's instructions and there must be documented internal procedures to ensure it remains in working order (primarily, but not exclusively an IM responsibility).

13.9 Secure disposal or re-use of equipment

13.9.1 Where a computer or media device must be reused outside the team it was originally assigned to, all data on the equipment must be securely erased prior to re-assignment

13.9.2 Where a computer or media device has reached the end of its useful life, all data on the equipment will be securely erased and then disposed of in an environmentally friendly manner.

13.10 Deliveries of ICT equipment

13.10.1 Loading areas and holding facilities will normally be defined as enhanced secure areas

13.10.2 Deliveries of ICT must be signed for by an authorised individual using an auditable formal process.

13.10.3 Subsequent removal of equipment should be via a formal, auditable process

13.11 Regular audit

13.11.1 Information security arrangements will be audited regularly by an independent 3rd party

This policy will be monitored and reviewed by the Governors on an annual basis.

Policy updated: April 2020

Staff responsible: Sally Bacon

This policy was ratified by the Governing body/Local Authority on:

Signed on behalf of the Governing Body: _____(signature)

_____(Printed)