The John of Gaunt School

A Community Academy

Information (Data Handling) Security Policy

Originator	Reviewed by	Date of Review	Approved by	Date of Approval	Next Review Date	Website
SLICT	Audit Committee	26/11/2018	Full Board	10/12/2018	December 2020	Yes

Table of Contents

1. Vision Statement

'Creating an irresistible climate for achievement'

We challenge, support and encourage every student to **achieve their potential**.

- We believe **effort** and **dedication** lead to success and we **raise aspirations**.
- We **personalise our provision** to meet the needs of individuals.
- We enable our students to flourish as **confident learners and leaders** of our community.
- We create a culture where all stakeholders **feel valued, supported and proud.**
- We **work collaboratively** to improve outcomes for our students and support other schools to improve.

2. Introduction

The John of Gaunt School issues this policy to meet the requirements incumbent upon them under the [i]Data Protection Act 2018 for the handling of personal data in the role of controller.

The John of Gaunt School processes large amounts of personal and confidential information on its consumers, and has a responsibility to maintain privacy and security regarding this information. To this end the **confidentiality**, **integrity**, **availability** and **accountability** of this information needs to be protected from harm in a way that is proportionate to the risks to the information.

The purpose of this policy is:

- To protect the organisation's information and subsequently to protect the organisation's reputation
- To enable secure information [ii]sharing to deliver services
- To protect the organisation from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the organisation's employees

3. Scope

This policy applies to all employees of The John of Gaunt School including contract, agency and temporary staff, volunteers and employees of partner organisations working for The John of Gaunt School whenever and wherever that they process the organisation's information.

The policy applies to all forms of information including, but not limited to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled The John of Gaunt School, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio
- Written on paper or printed out from a computer system. This may include working both on-site or remotely (e.g. at home)
- Stored in structured manual filing systems
- Transmitted by email, over the Internet, fax (if in place), and via wireless technology
- Stored and processed via computers, computer networks or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

4. Legal Principles

In execution of this policy, The John of Gaunt School will comply with the data protection principles of the Data Protection Act 2018. Specifically the principle that personal data is *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

The John of Gaunt School will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures.

5. Roles & Responsibilities

All consumers which include staff, contractors, consultants, suppliers, volunteers, governors and trustees must:

a) Be familiar with this policy and other relevant policies and procedures including, but not limited to:
   i. Data Protection Policy
   ii. Breach Notification Procedure
   iii. Records Management Policy with Retention Summary
   iv. Staff & Students Acceptable Use Policy
b) Play an active role in protecting information in their work
c) Read and act on any training and awareness, and communications regarding information security and ask for clarification if these are not understood
d) Take care when handling information to ensure it is not disclosed to those without the need to know or are not approved
e) Report any breaches, near misses, or incidents to the organisation via the organisation's Data Breach Policy and procedures

Governors and Senior Leaders are required to:

a) Approve this policy
b) Actively promote a culture of privacy and security
c) Ensure security and privacy is considered throughout the development of any new service, process or product
d) Cascade any relevant communications regarding information security
e) Ensure Information Owners are assigned for its sensitive data held by the school – (Appendix 4)

Ultimately, this group are accountable for the organisation's information, therefore there may be other elements that this cohort deliver as part of their roles.

Information owners are required to:

a) Update the organisation's Data Audit Spreadsheet *(Record of Processing Activities-Information Audit)* at least on an annual basis
b) Contribute to the risk assessment on their information assets, and own the risks, the potential mitigations, and the implementation of any controls
c) Ensure Business Continuity Plans are in place for their information assets as well as being exercised / tested
d) Be involved in any investigation regarding breaches, incidents or near-misses associated with their information assets

ICT are required to:

a) Be the custodian of electronic systems which process information assets
b) Assist information owners and the Data Protection Officer in identifying any risks associated with the processing of information on the organisation's electronic systems
c) Assist from a technical level with any investigation regarding breaches, incidents or near-misses associated with the organisation's information assets

d) Report any unauthorised access, or unauthorised access attempts to information systems
e) Ensure software and operating systems are appropriately licensed

[iii]**Data Protection Officer(i-West,** i-west@bathnes.gov.uk **)** is required to:

a) Monitor compliance with Data Protection Law and this policy, reporting this to the Senior Board
b) Assist the organisation with any Data Protection Impact Assessment which could include recommending controls to reduce risk
c) Assist the organisation with any queries they have regarding data protection

6. Data Protection by Design

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity i-west must be consulted and an initial screening be conducted assessing risk.

The concept of *data protection by design* will be a guiding principle in achieving the security of individual's data protection rights. The following will be considered as part of data protection by design

- **Encryption** – the use of strong cryptography to protect data at rest and in transit
- **Pseudonymisation** – the use of a unique reference number
- **Data Minimisation** – information is only personalised or personally identifiable for the minimum amount of time and only until the purpose is achieved

Any activity involving the processing of personal data must be registered on the Register of Processing Activity (Information Inventory / Audit) and reviewed at the very least annually.

7. Bring Your Own Device

Student Owned Devices – **Mainly Year 12 &13 and some SEN students**

The School has implemented a scheme whereby students may undertake study using their own, school - approved, mobile devices.

- Such devices remain the property of the student, and they, together with any other personal devices using the school system, are restricted through the implementation of technical solutions that provide appropriate levels of network access;
- Personal devices are brought into the School entirely at the risk of the owner;
- The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or in use on activities organised or undertaken by the School;
- The School recommends insurance is purchased to cover that device whilst out of the home;
- The School accepts no responsibility for the day to day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues;
- The School recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the School
- Pass-codes or PINs must be set on personal devices to aid security;
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements;
- Users must log out of programmes when they are not in use;
- Passwords must not be saved, for example to the browser history;
- Devices may not be used in public or mock examinations;

Staff Owned Devices

- Staff must not use their own devices to take images of students.
- Only school equipment may be used and images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
- Staff should not save the personal numbers of students to their devices, and should use trip phones where appropriate
- Pass-codes or PINs must be set on personal devices to aid security; and where possible encryption applied to the device.
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements;
- Users must log out of school programmes and applications when they are not in use;
- The device must have the latest updates applied;
- Passwords must not be saved, for example to the browser history;
- Users must not download data locally to the device (e.g. email attachments)

8. Procedures

Appendix 1 includes procedures to aid consumers protecting the organisation's information assets.

9. Security Incidents

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the organisation and the Data Protection Officer (i-West, i-west@bathnes.gov.uk) must be informed immediately and the Data Incident Reporting Form completed. The form is designed to manage, investigate, report and provide 'Learning from Experience' (LFE) to avoid future incidents occurring.

In any case an incident must be reported no later than 24 hours from identification, except where a malicious incident has occurred. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Procedures

10. Discipline

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the Head teacher, shall take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;
Change of Data Protection Administrator,
Change of Legislation

Appendices

Appendix 1 – Information Security Procedures

All consumers must protect personal data at rest by applying appropriate security:

1) **Locking screens** when away from their desks (using ⊞ +L)
2) By **disposing of information and equipment** in an appropriate manner:
   a. Equipment – via the organisation's accredited provider
   b. Paper – using either a crosscut shredder or the organisation's accredited provider which may be facilitated by Confidential Waste receptacles.
3) Ensuring **special categories of personal data**[1] is given extra security, and at a minimum is locked away when not in use ([1] *race/ethnicity, religion, genetics, health, photos, sexual orientation, trade union, political opinions*)
4) Using encryption when **processing personal data offsite** e.g. working at home (either on an encrypted device or an encrypted USB stick owned by the organisation). For encrypted sticks users must
   a. ensure the information is uploaded back to the organisation's network as soon as possible, and;
   b. only process the data on the stick and not process or save the data outside of the stick (e.g. locally to the device).
5) When processing data on an unmanaged (**personal device**) users must ensure:
   a. The device is protected by PIN, Password or fingerprint, and ideally encrypted
   b. That the organisation's systems (e.g. Webmail) are not left logged in
   c. That attachments are not opened (and downloaded), unless in an emergency where measures are to be taken to delete the information after use
6) **Data taken offsite must be protected at all times**, as well as the above, users must:
   a. Keep information and equipment on their person at all times (e.g. when stopping off on the way home)
   b. Be held in an appropriate receptacle (e.g. bag) to reduce the risk of opportunistic theft
   c. Not store leave the information and equipment in a vehicle when not in use
   d. Consider whether data minimisation could be used. For example:
      i. Not making the information personally identifiable, by using pseudonymisation (e.g. Unique reference or initials)
      ii. Using a code system or colour code system to identify key indicators (e.g. allergies)
      iii. Not having the organisation logo on any hardcopy documents
      iv. Using encryption to protect the data (e.g. encrypted device rather than hard copies)
7) **Ensuring care is taken with emails**, by applying the following:
   a. Was I expecting this email?
   b. Does it look and feel right?
   c. Can I check (by other trusted means) that the email is legitimate?
   d. Not clicking any links or opening any attachment with validating them
   e. Using blind copy (BCC) when emailing more than one external user
   f. Double checking the email address when sending emails
   g. Encrypting personal data to external addresses (See Appendix 3)
   h. A one minute email delay rule is in place on all emails sent, this provides a safety net where all emails sent are held in Outbox for one minute before delivery allowing the user to edit/delete (See Appendix 2)
8) Ensuring any **information disclosed verbally** is
   a. Validated – the person calling/present is known to have the need to know
   b. Documented – a summary of what was disclosed and filed
9) Ensuring any **information sent via post has the address double checked** – where possible copy and paste from a system and is marked Private & Confidential

Appendix 2 – Setting up an email delay (in Outlook 2013)

This can either be setup by a user or, with the aid of the organisation's IT Team, can be setup corporately.

1. Click the **File** tab.
2. Click **Manage Rules and Alerts**.
3. Click **New Rule**.
4. In the **Step 1: Select a template** box, under **Start from a Blank Rule,** click **Apply rule on messages I send**, and then click **Next**.
5. In the **Step 1: Select condition(s)** list, click **Next**.

   If you do not select any check boxes, a confirmation dialog box appears. If you click **Yes**, the rule that you are creating is applied to all messages that you send.
6. In the **Step 1: Select action(s)** list, select the **defer delivery by a number of minutes** check box.
7. In the **Step 2: Edit the rule description (click an underlined value)** box, click the underlined phrase **a number of** and enter the number of minutes for which you want the messages to be held before sending.

   Delivery can be delayed up to 120 minutes. I would suggest 1 or 2 minutes.
8. Click **OK**, and then click **Next**.
9. Select the check boxes for any exceptions that you want.
10. Click **Next**.
11. In the **Step 1: Specify a name for this rule** box, type a name for the rule.
12. Select the **Turn on this rule** check box.
13. Click **Finish**.

After you click **Send**, each message remains in the **Outbox** folder for the time that you specified.

Appendix 3 – Securing an email in transit

The three main risks associated with email are:

1) Emails are intercepted in transit
2) Emails are sent to the wrong recipient
3) Email addresses are disclosed to those without the need to know

This process covers risk (1) and enables the secure exchange of information over email (in the absence of a secure email portal).

1) Document the information in an MS Office document
2) Ensure that this is not the source/primary document – if it is then create a copy

   Do not encrypt the source document – if you do, and forget the password you are unlikely to be able to gain access to the information again!
3) Have the document open, and then click
   a. File
   b. Protect Document
   c. Encrypt with Password
   d. Create a strong password (minimum of 8 characters) – you could use a password generator https://passwordsgenerator.net/ or pre-agree one with the recipient
   e. Apply this password to the document
   f. Save
4) Attach the secured document to an email and send it to the recipient
5) Communicate the password by other trusted means e.g. Phone call, or message. Before telling them the password ensure you:
   a. Are communicating with the correct person; and
   b. Confirm that they have received the email

      It should be noted that encrypted attachments are sometimes blocked by email gateways as they cannot inspect the contents

Appendix 4 – Register of sensitive data held by the school [iv]

(This register will be sent to all staff each year to allow colleagues to revise the list of types of data that they hold and manage)

Type of data, main person responsible	**Held on**	**Reason for collecting this data**	**Period to be retained**[1]	**Type of protection**	**Who can access the data**
Pupil - SEN data **SENCO**	SIMs database Paper files/copies	To allow staff to access information which will facilitate deployment of appropriate teaching and learning strategies. To create an accurate provision map and enable progress tracking	DOB of child + 25 years	Two-factor authentication Locked in filing cabinet in locked Office. CCTV Building	Teaching Staff and staff identified by SENCO as needing the required permission in SIMs
Pupil - Child Protection data **Designated Person responsible for Child Protection**	Safeguarding System	Legal requirement - essential records on safeguarding issues and welfare	DOB of child + 25 years	Full encrypted data. Accessed via separate system on different server. Backed up each evening - in new system to be backed up to UK based cloud system - also encrypted. Full system audit of all keystrokes entered on system.	Administrator rights - Senior designated person and Deputy DSP. User access given to those who need to update the system. Currently only Student Development team,(Inc Sarah Smallbone), Head Teacher and Head Teacher's PA. Access only through password login.
Pupil - New Starter Application Forms	SIMs database Paper files/copies		As above if successful or until appeals process is complete	Two-factor authentication Locked 2nd floor Office.	3 Administrators with Keys to the Data Office

Data Manager				CCTV Building	
Staff - HR data **HR & HR Assistant**	SIMs database Paper files/copies		Termination of Employment + 6 years *(please refer to HR documentation for specific retention periods as these vary depending on circumstances)*	Two-factor authentication Locked 2nd floor Office. CCTV Building	4 Staff with access to these files HR & HR Assistant Head Teacher and Head Teacher's PA.

Appendix 5 –Timetable for Information Security Management

(The audit will be completed by a member of staff responsible for data protection)

Activity	**Frequency**	**Lead**
Audit of data held	Annually	Head and SIMs/Database Manager
Encrypting sensitive data	On-going	All staff
Data backup	Daily	ICT Technician
Reviewing data backup procedures	Annual	ICT Technician & SIMs/Database Manager
Identifying staff responsible for data security and keep log of names and roles.	Annual	SIMs/Database Manager
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

Appendix 6 - Staff Computer Use Policy

This policy is reviewed every two years or as necessary

Staff Computer Use

- Passwords that I use to access school systems will be chosen sensibly and kept secure and secret – if I have reason to believe that my password is no longer secure I will change it.
- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web content or use pictures or text that can identify the school, without the permission of the Headteacher.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school. I will seek permission with the school's technician / Network Manager should I need to install additional software.
- I will always adhere to copyright legislation.
- I will always log off the system when I have finished working.
- I understand that the school may, in line with compliance with legal obligations, monitor the Internet sites I visit.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager / school technician / headteacher.
- Any e-mail messages I send will not damage the reputation of the school.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be forwarded.
- I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- I understand that I am responsible for the safety of school data that I use or access.
- In order to maintain the security of data I will take the following steps:
    - I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.
    - I will not save data files to a PC or laptop other than that provided by the school.
    - If I need to transfer sensitive data files and no secure electronic option is available I will only do so using the encrypted USB key provided by the school.

- Sensitive data will only be sent electronically through a secure method, e.g. Perspective. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

  Sensitive data includes:
  - Pupil reports
  - SEN records
  - Letters to parents
  - Class based assessments
  - Exam results
  - Whole school data
  - Medical information
  - Information relating to staff, e.g. Performance Management reviews.

If I am in any doubt as to the sensitivity of data I am using, I will consider these questions:

- Would disclosure / loss place anyone at risk?
- Would disclosure / loss cause embarrassment to an individual or the school?
- Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could be recorded on any future Criminal Record Bureau checks.

Name…….

Date……..

References:

[i] Data Protection Act 2018

[ii] Information sharing: advice for practitioners providing safeguarding services

[iii] Data protection: toolkit for schools

[iv] Information Management Toolkit for Schools

Information Commissioner's Office