GEORGE WATSON'S COLLEGE

Information Security:
Information Handling Policy

Introduction

This Policy sits below the George Watson's College ("the School") **Overarching Information Security Policy**. It sets out the additional principles, expectations and requirements relating to the handling of the School's information assets.

1. Purpose

Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability and non-compliance with legislation, e.g. GDPR, which would otherwise occur.

2. Scope

This Policy applies to all members of staff, which includes Governors, volunteers, peripatetic teachers and also third parties with access or responsibility for storing and managing School data.

3. Policy Statement

3.1 Definition of an Information Asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and life cycles.

When identifying information assets, the following questions are considered:

- Does the information have a value to the organisation?
- How useful is it?
- Will it cost money to reacquire?
- Would there be legal, reputational or financial repercussions if you could not produce it on request?
- Would it have an effect on operational efficiency if you could not access it easily?
- Would there be consequences of not having it?

Generally speaking, it enables or improves the operation of the School. The following areas are a few illustrative examples of our information assets.

- School strategies, plans, goals and objectives
- Training and educational materials
- Management Information System (MIS), i.e. PASS/3Sys data, Raiser's Edge
- Marketing media - such as an advertising banner or video used to generate demand or brand awareness
- Google application that hosts data which is critical to the operation of a department or the wider School. Data about parents, prospective parents and former pupils
- Financial information such as accounting data and financial reports which may not be in the public domain.

3.2 Inventory and ownership of information assets

An inventory of the School's main information assets will continue to be developed and maintained and the ownership of each asset clearly stated. Due to the extensive volume of information assets across the School and

the changing nature of information, this will require regular reviews of all organisational areas and information asset owners.

Each asset will have a nominated owner in the Principal's Leadership Team (PLT) and they will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it.

3.3 Security classification

Security classification is not yet in place. Recommended practice would be to label all data/information assets with one of the four categories below:

- Public – available to any member of the public without restriction, e.g. general website content
- Internal - available to staff, pupils, contractors and volunteers, e.g. timetable, music school timetable, teaching materials, technical guides, etc.
- Confidential - confidential information available only to specified staff, pupil or parent with appropriate authorisation, e.g. Accounts data, Pupil disciplinary records
- Highly Confidential – available to only a very small number of staff with appropriate authorisation, e.g. Guidance or Support for Learning information, medical data, protected characteristics, Payroll/HR data, etc.

Any information which is not explicitly classified would be classified as public, by default.

3.4 Access to information

Users will be granted access to the information they need in order to fulfil their roles within the School. Users who have been granted access must not pass on information to others unless those others have also been granted access through appropriate authorisation.

3.5 Disposal of information

Information assets must be disposed of securely.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the School, unless the disposal is undertaken, under contract, by an approved contractor.

Electronic waste, IT equipment such as mobiles, laptops and screens must be disposed of in accordance with IEEE regulations. IT Services will ensure that all data and information assets held on these devices are securely destroyed and that a certificate of secure destruction is held centrally within IT Services.

Confidential paper waste must be disposed of in accordance with School procedures.

3.6 Removal of information

School data that would be classified as Internal or above should be stored using School facilities or with third parties subject to a formal, written legal contract with the School, wherever possible. In cases where it is necessary to otherwise remove data from the School, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

Particular care needs to be taken when information assets are in transit. School supplied mobile devices must always be password protected and encrypted where possible, and confidential or highly confidential information should never be stored locally on these devices. Only secure home drives, Google drives or secure systems should be used to store this information.
Staff are not permitted to copy, migrate or transfer data to personal accounts. Everyone has a responsibility to protect School data from unauthorised access and take necessary precautions when storing, transferring or transmitting school data.

3.7 Using personally owned devices

Any processing of School information using personally owned devices must be in compliance with the School's **Acceptable Use Policy and Mobile and Remote Working Policy.**

3.8 Information on desks, screens and printers

Members of staff who handle confidential paper documents must take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents must be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers must be locked while unattended.

Passwords must never be written down and left in plain sight, nor shared or divulged to others.

3.9 Backups and restoration

Asset owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Information which is entrusted to the care of IT Services will meet these requirements. The asset owners will be responsible for testing restoration and recovery of the business services on a regular basis.

3.10 Data retention

All data must be retained and securely disposed of in accordance with the stipulations of the **Data Retention and Storage Policy.**

3.11 Exchanges of information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. This should include a signed agreement, the School's bilateral NDA and/or a Data Sharing Agreement, whichever is most suitable for the purpose.

Regular exchanges of information must be covered by a formal written agreement with the third party.

When exchanging information with external organisations by email, recipient addresses should be checked carefully prior to transmission. If email is required to send confidential information then it should be sent via the EGRESS system. IT Services can help enable this service for those who require it.

Highly confidential and Sensitive information must never be shared with colleagues via Email. The School's MIS systems should always be used.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

No one must disclose or copy any information classified as Internal or above unless they are authorised to do so.

Everyone should check carefully before sending any information due to the vast amount of phishing and corrupt websites trying to obtain valuable information. It is everyone's responsibility to maintain security of the School's data and undertake compulsory Information Security training on a regular basis.

3.12 Reporting losses or Data Breaches

All staff have a duty to report the loss, suspected loss, unauthorised access or suspected unauthorised access of any School information, system or process, to the IT Services via it-support@gwc.org.uk and to the Data Protection Officer via email to **dataprotection@gwc.org.uk** as soon as they become aware of the breach. Appropriate steps will be taken to ensure that School data is secured, the incident or breach is logged and guidance is provided on the procedural steps necessary to resolve the incident and minimise the impact as quickly as possible.

Further information is available within the **Security Incident Management Policy and Procedure.**

4. Implementation

This Policy will be posted on the School's Staff Portal and be made available to all users.

PLT and all those with line management responsibilities are responsible for ensuring all members of staff understand and comply with this Policy.

5. Policy Compliance

5.1 Compliance Measurement

The IT Services Department will verify compliance to this policy through various methods, including but not limited to, business reporting tools, internal and external audits, system monitoring and feedback to the Head of IT Services as Policy Owner.

5.2 Exceptions

Any exception to the policy must be approved by the Head of IT Services, in advance.

5.3 Non-Compliance

Non-compliance with this policy could result in disciplinary action in line with the School's Disciplinary Policy and Procedure.

6. Review, Approval and Governance.

This Policy will be reviewed at least every two years by the Head of IT Services.

The Principal's Leadership Team is the Approval Body for this Policy.

Owner	Title	Date	Signature
Karen McPhillips	Head of IT Services	Aug-23	Karen McPhillips

Approved By	Title	Date	Signature
Su Breadner, on behalf of PLT.	Chief Operating Officer	September 2023	

Version	Date last reviewed	Reviewer	Notes
V1.0 DRAFT	07/01/2020	Karen McPhillips	Initial draft complete

V0.2 Draft	25/01/2021	PLT (KG)	PLT approved 22/01/2021
V0.21 Draft	04/07/2023	KM/SC	Very little change from V0.2
V0.22 Draft	11/08/2023	KM	A few minor amendments; stating staff must undertake compulsory training, Added statement around protecting and not transmitting or transferring school data
V0.23 draft	8/9/2023	SB	Small change to line management responsibility clause

Owner	Title	Review Date	Review Completion Date
Karen McPhillips	Head of IT Services	July-23	13th August 2023
Karen McPhillips	Head of IT Services	Aug-25	