GEORGE WATSON'S COLLEGE

Information Security:

Overarching Policy

Introduction

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as George Watson's College ('The School') where information relates to learning and teaching, administration and management. This policy is concerned with the management and security of the School's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to the School) and the use made of these assets by its members and others who may legitimately process school information on behalf of the School.

This overarching policy provides an overview of information security and lists a hierarchical set of policy documents (sub-policies), which, taken together, constitute the Information Security Policy for George Watson's College.

The General Data Protection Regulations (GDPR) require organisations to process personal data securely. The GDPR Security Principle states that personal data shall be:

"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"

This is not a new data protection obligation, it replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR provides more specifics covering what we have to do about the security of our processing and how we should assess our information risk and put appropriate security measures in place. Whilst these are broadly equivalent to what was considered good and best practice under the 1998 Act, they are now a **legal requirement**.

1. Purpose

This Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. Adhering to the principles is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

2. Scope

The sub-policies in the Information Security Policy apply to:

- All **information assets** which are owned by the School, used by the School for business purposes or which are connected to any networks managed by the School
- All **information** which the School processes, irrespective of ownership or form
- All **staff** of the School and any others who may process information on behalf of the School.

Some of the sub-policies apply to users of the School systems and are relevant to **protect** the services provided, the individual user and the School's reputation.

3. Structure

This top level document lists a set of sub-policy documents which together constitute the Information Security Policy for the School. All of these documents are of equal standing, although this suite of policies should be internally consistent for the removal of any doubt. If any inconsistency is found between this overarching policy and any of the sub-policies, the overarching policy will take precedence.

Each of the sub-policies only contains high-level descriptions of requirements and principles. They do not, and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policies.

4. Policy Statement

4.1 Information Security Principles

The School has adopted the following principles which underpin this policy:

- Information will be protected in line with all relevant School policies and legislation, notably those relating to data protection
- Each information asset will have a nominated owner in the Principal's Leadership Team (PLT) who will be assigned accountability for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset - See **Information Asset Register**
- Information will be made available solely to those who have a legitimate need for access
- The integrity of information will be maintained
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification
- Information will be protected against unauthorised access
- Compliance with the Information Security Policy will be monitored.

4.2 Governance

Responsibility for the production, maintenance and communication of the overarching policy and all sub-policies resides with the Chief Operating Officer.

This overarching policy has been approved by the Principal's Leadership Team (PLT). Substantive changes may only be made with the further approval of PLT.

Responsibility for the approval of the sub-policies is delegated to the Chief Operating Officer. Before approving any sub-policy, PLT, IT Services and/or other School managers, members of the Governing Council and employee groups, as appropriate, will be consulted.

4.3 Monitoring

Use of the School's computing systems and platforms, including Email and Internet use, will not, as a matter of course, be monitored. However, the School may implement monitoring in certain circumstances where it has reason to believe that misuse is occurring. See **Investigation of Computer Use Policy.**

4.4 Implementation

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

PLT, Deputy Heads, Heads of Department and line managers are responsible for ensuring all members of staff understand and comply with this Policy.

Regular and compulsory IT Security training will be provided to all staff on an annual basis and all staff will be expected to complete and understand their obligations and high-level security responsibilities. The same compulsory training will be provided to all new staff.

5. Sub-Policy Document List (by audience)

INFORMATION SECURITY POLICIES	
All Users	**IT Services**
Mobile and Remote Working Information Handling Investigation of Computer Use Security Incident Management Email Use Internet Use Software Management Acceptable Use (Staff) Acceptable Use (Pupils P1 - P4) Acceptable Use (Pupils P5 - S6) Device Loan Agreement (Pupils S1-S6) Device Loan Agreement (Pupils P1-P7) Password Policy Hardware Replacement Retirement and Redeployment Policy Information Asset Register	IT Professionals' Policy GWC IT Code of Conduct Third Party Network Access Privileged Access Data Loss Prevention Encryption

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.

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 and Approval

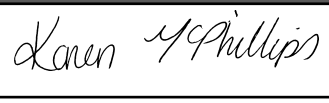
The documents constituting the Information Security Policy will be reviewed at least every two years or when key changes or new/amended legislation is introduced.

It is the responsibility of the Chief Operating Officer to ensure that these reviews take place and to ensure that all the relevant policies remain internally consistent. The review will be undertaken by the Head of IT Services.

Changes or additions to the Information Security Policy may be proposed by any member of staff via their Head of Department or line manager, to the Chief Operating Officer.

Substantive changes made to any of the policies will be communicated to all relevant staff/users.

The Property and Facilities Committee of the Governing Council is the Approval Body for this Policy.

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

Approved By		Date	Signature
Property and Facilities Committee	COO (on behalf of Property Committee)	Sept-23	

Version	Date last reviewed	Reviewer	Notes
V1.0 DRAFT	20/05/2020	Karen McPhillips	Initial draft complete
V0.2 Draft	11/12/2020	KM, SC & KD	Final Review - Only IAR agreement with PLT
V0.3	25/01/2021	PLT (SB, KG & GB)	Approved at PLT 22/01/21
V0.31	04/07/2023	KM, SC	Only very small grammatical changes from V0.3
V0.32	09/08/2023	KM	Minor changes to the introduction, review of the scope with COO. Reference to information assets is new. Change to implementation to include new staff.

Owner	Title	Review Date	Review Completion Date
Karen McPhillips	Head of IT Services	Aug-23	9th August 2023
Karen McPhillips	Head of IT Services	Aug-25	