Information Security Policy

Last Updated: March 2018
To be Reviewed: March 2020

Information Security Policy

1. Introduction

1.1 Information Security
The availability of complete and accurate information is key to providing excellent services to the pupils, parents and staff of Hamilton College. The school holds and processes a large amount of confidential and personal information on private individuals, employees, service partners, suppliers and its own operations. Hamilton College has a number of responsibilities to protect their reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the confidentiality, integrity, availability and accountability of this information need to be protected from harm in a way that is proportionate to the risks to the information. This Information Security Policy provides the overall framework to help everyone play his or her part in protecting pupil, staff and other stakeholder information.

1.2 Scope
The Information Security Policy applies to everyone who reads or processes school information. The policy applies wherever and whenever school information is processed and applies equally to all users including:

- Teachers, Support Staff, Music tutors, Sports coaches, Educational Psychologists and Governors
- Contractors, consultants, casual and temporary employees and volunteers
- Partners and suppliers

Please note that throughout this document, the words “employee” and “user” are used to cover all the groups of people listed above. The Information Security Policy applies to all forms of information, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned, administered or controlled by Hamilton College, 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 onsite or remotely (e.g. at home)
- Stored in structured manual filing systems
- Transmitted by electronic mail, fax, over the Internet 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.

1.3 Purpose
The purpose of the Information Security Policy is:

- To protect the School’s Information and subsequently to protect the School’s reputation
- To enable secure information sharing to deliver services
- To protect the School from legal liability and its systems from 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 School's employees, NOT to constrain reasonable use of information in support of normal business activities of the School
- This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

1.4 Breaches of the Information Security Policy
Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious. Breaches of this policy by a user who is not a direct employee of the School may result in action being taken against the user and/or their employer. In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated. Breaches of the Data Protection Act 2018 and General Data Protection Regulation 2016 could result in a fine being issued to the individual and/or the organisation.

2. Information Security Roles and Responsibilities

2.1 All information users including employees, contractors, consultants, volunteers, governors, partners and suppliers must:

1. Comply with this Information Security Policy and where appropriate, the Staff ICT Acceptable Use Policy.
2. Comply with legal, statutory, regulatory and contractual obligations related to information at all times.
3. Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to confidentiality, integrity and availability.
4. Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.
5. Report immediately all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the School's information or information systems, following agreed incident management policies and processes.
6. Read and act on any communications and training about information security and ask for clarification if these are not understood.
7. Play an active role in protecting information in day-to-day work.

2.2 Governors and School Senior Leadership Team

1. Approve this Information Security Policy.
   Actively promote effective and appropriate information security by the use of structured risk assessment in all future developments and by appropriate retrospective risk assessment of current processes and systems.
2. Implement and promote Information Security to all staff.
3. Ensure that employees understand and abide by the Information Security Policy and its associated policies, processes, procedures, guidelines and understand its impact.
4. Assign owners to all information in their area of responsibility.
5. Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.

6. Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
7. Provide written authorisation for access to information.
8. Ensure that communications regarding information security are cascaded effectively to all staff.
9. Ensure that information security is an integral part of all departmental processes.

2.3 Information owners

1. Data sets may have different owners and where several potential information owners exist, responsibility should be assigned to the manager whose group makes the greatest use of the data.
2. Use structured risk assessment to select security controls to protect their information.
3. Monitor to ensure security controls continue to be effective and that information is being handled correctly.
4. Report and act on security incidents and weaknesses relating to their information according to agreed incident management policies and processes.
5. Manage the residual risks to their information.
6. Prepare appropriate Business Continuity plans and contingency arrangements.

2.4 IT Support Staff

1. Be the custodian of electronic information in its care by implementing and administering technical security controls as specified in the information security policies, and by the Information Owners as a result of information security risk assessment.
2. Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
3. Ensure all software is licensed and remove unlicensed software.
4. Provide contingency arrangements for information systems.
5. Provide appropriate protection from malicious software.
6. Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
7. Monitor and investigate technical security breaches.
8. Provide technical support to enable compliance with this policy.

3. Information Security Policy

3.1 The School operates within the law at all times

1. Information shall be used legally at all times, complying with UK and European law. All users, including employees, and agents of the School might be held personally responsible for any breach of the law.
2. All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the Data Protection Act 2018 and General Data Protection Regulation 2016. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the School without proper authorisation.
3. Personal, confidential or sensitive information shall be protected appropriately at all times and in particular when removed from School premises either physically on paper or electronic storage devices, or when transmitted electronically outside the School.
4. Personal, confidential or sensitive information shall not be included in the text of e-mails to be sent outside the organisation, or in files attached to them, unless these

are securely encrypted or sent by secure network links. Please be confident that the link is secure before this is used. Hamilton College has an email encryption solution in place for designated members of staff and this should be used effectively.

5. Any request for information under the Data Protection Act shall be handled in accordance with the law and processed within 20 working days.
6. Information shall not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.
7. The School shall only use licensed software in accordance with the related license agreement.
8. Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright.

3.2 Access to information shall be controlled

1. The requirements for confidentiality, integrity, availability and accountability shall be determined for all information, from creation to deletion.
2. Access to information shall be authorised by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required before access is granted to certain information systems and facilities.
3. Information users shall not attempt to access information to which they do not have authority. If users were to find themselves in a position where they have access to information, whether via physical or electronic, which they knowingly should not, they should not access this information. Further, they should report this insecurity to a member of IT support staff and SLT. Unintentional insecurities to information do not constitute authorisation for access.
4. Information users shall keep personal passwords confidential at all times.
5. External business partners and suppliers with whom we have an agreement or contract shall be required to sign a Data Processing Agreement, where appropriate.
6. All equipment, including network equipment, attached to the School's computer network shall be approved by the IT Manager before connection.
7. School equipment, facilities and information shall be used only for the School's business purposes, unless written permission of SLT has been obtained. School equipment, facilities and information should not be used for personal gain or profit.
8. All information about the security arrangements for School computer and network systems and structured manual filing systems is confidential to the School and shall not be released to people who are not authorised to receive such information.

3.3 The availability of information shall be protected

1. Business continuity plans shall include all aspects of the School's infrastructure, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.

3.4 The integrity of information shall be maintained

1. A named individual should have operational responsibility for the ICT systems and procedures.
2. The accuracy and completeness of information, including structured manual filing systems, processing methods and computer software shall be protected from unauthorised modifications. Users shall not attempt unauthorised modifications.
3. Users shall use only the officially provided or approved facilities and systems to access School information.
4. Users shall not interfere with the configuration of any computing device without approval.
5. Update regularly all devices, which are subject to the threat of malicious software, with malicious software scanning software.
6. Update regularly all devices, which are subject to the threat of security vulnerabilities with appropriate security patches.

4. Monitoring of the Information Security Policy

The use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure that this policy is adhered to and to detect and investigate unauthorised use of information.
- To maintain the effectiveness, integrity and security of the computer network.
- To ensure that the law is not being contravened.
- To protect the services provided by the organisation to the public and protect the integrity and reputation of the organisation.
- All monitoring shall be:
    - Fair and proportionate to the risks of harm to the School information and reputation.
    - Undertaken so as to intrude on users' privacy only as much as is necessary.
    - Carried out subject to the requirements of legislation, e.g. Regulation of Investigatory Powers Act 2000. Access to any records of usage shall be stringently controlled.

5. Review of the Information Security Policy

This policy shall be reviewed on a regular basis and at least every two years. This policy and its associated policies, processes, procedures and guidelines shall be updated according to:

- Internally generated changes e.g. changes in service strategy, organisation, locations and technology
- Externally generated changes e.g. changes in legislation, security threats, security incidents, recommended best practice and audit reports
- All changes shall be approved by the Principal and School Governors and be made available to everyone to whom it applies.