HARLOW COLLEGE

INFORMATION SECURITY POLICY

Introduction

Information security is essential to ensure effective data sharing and to support the college's academic and corporate objectives.

The following principle applies in the management of Information Security:

Data, whether stored electronically or on paper, in transit or in use, is protected from unauthorised use and disclosure to ensure the required levels of confidentiality, integrity and accessibility and compliance with legislation.

Scope

This policy applies to all information and Information Systems owned by the College, including information and systems maintained by third parties on behalf of the College and personally owned electronic equipment and storage equipment chosen to be used by individual members of staff in their work. Information may be electronic, paper, verbal or other.

Responsibilities

Governance

- The SMT ensures that IT security is properly evaluated and managed across the College. This policy is written, maintained, monitored and reviewed by the Principal and SMT.

Users

- Users of College information systems and networks will act responsibly and in full compliance with all relevant policies and procedures when handling and sharing College data, in whatever format (i.e. digital or physical) whether on College equipment or personally owned devices and storage equipment.

Third Parties

- Third parties who manage, process, transmit or store information or information systems on behalf of the college will act responsibly and in full compliance with this policy and all relevant policies and procedures when handling and sharing College data.

Principles

Information security measures protect information from a wide range of threats and safeguard based on the following security principles:

- **Confidentiality** – through protection from unauthorised access and disclosure.
- **Integrity** – by ensuring the accuracy and completeness of information and of processing methods.
- **Availability –** by ensuring that information and associated services are available to authorised users when required. Information exists in many forms and includes printed matter and electronic data, video, audio and text content.
- **Accountability:** Lawful and appropriate management of systems and data is not only a corporate responsibility but a personal one. Users will be held individually accountable for their own actions.

Whatever form information takes and however it is shared or stored, all College information will be appropriately protected.

With reference to the Laws and regulations in the References section the College will strive to ensure that:

- Information and its gathering systems comply with the law. This includes regulating access and could mean monitoring communications.
- Information content remains lawful. This includes checking data and software across College IT networks.
- Special care is exercised in managing personal and commercially confidential data.

This policy is brought to the attention of all members of staff and students and affiliated partners and staff. It is the responsibility of existing staff and students and all other users including contractors to check routinely the status of this policy, of updates and revisions and of other relevant College rules.

Information Security Actions

Risk assessment

Full risk assessments will be performed annually across College to address the vulnerabilities of information content and systems and current threats. The College Audit Committee reviews the effectiveness of risk management on behalf of the College. Heads of Academies are responsible for ensuring effective risk management of IT in their own areas.

Business Continuity

Information security forms part of wider business continuity planning within the College. Information security requirements will be regularly and routinely reviewed and reassessed accordingly.

Physical and environmental security

Appropriate security measures are installed and enforced to prevent unauthorised access, damage and interference to information and facilities. To prevent loss, damage or compromise of assets and disruption to business activities, information and equipment will be protected as far as possible from hazards. This includes reasonable protection against power failure and the establishment and maintenance of an offsite alternative operating centre.

Security of information systems

Rules for accessing College information facilities, the responsibilities of users and the rights of the College are set out in the College's IT service policies and procedures with which all staff and students are required to comply.

The following security measures are supported by the College to ensure the security of information and information systems:

1. Strong password controlled identity management for users and information systems

2. Proper authorisation and access control for users and information systems.

3. Appropriate encryption for information and subsequently the data in motion and rest.
4. Information and system backup and recovery.

5. Regular audit to ensure that only licensed and authorised software is used across IT in the college.

6. Adequate protection against malicious software and activities against IT in the college.
   - Users should recognise that inappropriate software interferes with the proper running of College systems and should not be installed or used without written permission. Installation of software can only be undertaken by the IT support team.
   - Any authorised software should be used only within the terms of its licence and should be properly maintained and upgraded.
   - College information must remain secure when it is taken or viewed away from College premises. Responsibility for data housed on mobile devices (notebooks, tablets, laptops, smart cards, USB devices, digital pens, mobile phones and so on) rests with the user in control of the device. Staff must take appropriate measures to secure both the data and the device.
   - The requirement for security of information outside the College applies equally to paper records and files.
   -
7. Through asset classification and control
   - To ensure effective asset protection the College will develop and maintain asset registers of hardware, software and information.
   - All information and systems should be labelled with relevant information classification, which will be defined in Information classification guideline.
   - A range of procedures and processes will be developed to support the systematic and secure handling of information assets across the College.

8. Through good working practices implemented and monitored at departmental levels:
   - A clear desk/ clear screen protocol where students have access. Where records are kept security should be in place in the form of access control or locks as appropriate.
   - Secure storage, including lockable filing cabinets and password protected computer files.
   - A nominated security officer to maintain data access lists and administer permissions.
   - Careful consideration about the best and most secure medium for
   - communication and retention of secure information.

Requirements for retention and disposal of information

Retention and disposal rules are addressed in the College Records and Archive Management Policy and related documents including the College Disposals Schedule. Appropriate procedures for information disposal should be made at departmental level with support.

Confidential material (including personal data and commercially sensitive material) should be disposed of securely:

- Physical records should be shredded or incinerated,
- Digital data should fully erased, under advice from College Information Technology Services

.

Information security awareness
Information security awareness is vital and the College will make every effort to ensure that users of information systems are informed and updated about best practice and current risks.

All users of College information and information services (including contractors) will receive appropriate information about College security standards.

Dedicated training and support is available particularly for users with special responsibility for creating and managing information.

Consequences
Failure to comply with this policy is a breach of College Regulations and may lead to appropriate sanctions. Staff and students will be subject to the College's disciplinary procedures. In some instances breach of this policy may also be a breach of the law.

Reporting
Speedy reporting of security incidents is vital to minimise loss and damage. College reporting procedures are as follows:

- Physical security incidents (vandalism, theft and so on) or suspicious behaviour should be reported at once to the 24-hour security desk on each campus.
- Physical software breaches (theft, overwriting, unauthorised access to data etc.) should be reported through the Head of the relevant department or service area to the IT Service and Data Controller.
- Information theft, manipulation or illegal access should be reported to the Head of the relevant department or service area to the IT Service and Data Controller.
- Mechanisms will be in place to monitor and quantify security incidents and to identify recurring breaches.

References
- The Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Data Protection Act 1998
- The College's Data Protection Policy
- The law in relation to obscene publications, defamation, harassment
- JANET Acceptable Use and Security Policy

TRACKING and REFERENCE INFORMATION
Date Approved: July 2014
Review Date: July 2017
Author/Responsibility: Director of Information and Clerk to the Corporation
Equality Impact Assessment: 3 March 2015
Date Agreed by Unions and/or Other Staff Representatives (if applicable): n/a
List of related policies, procedures and other documents: Staff Disciplinary Policy Guidelines for Managers: handling disciplinary issues Complaints Procedure Equality & Diversity Policy Equality and Diversity Scheme Grievance Procedure Guidelines for Managers: handling grievance issues Guidelines for staff on avoiding false accusations (folder: 'Guiding Principles') Data Protection Policy Safeguarding Policy Disciplinary Policy & Procedure for Senior Post Holders (SPH) Guidelines for Managers & Governors: handling performance issues for SPH's Guidelines for Managers & Governors: handling disciplinary issues for SPH's
Complaints: If you wish to submit a complaint about the application of this policy or the procedure of it, please send your request in accordance with the provisions of the Grievance Procedure.
Monitoring: The application of this policy and associated procedure will be monitored by HR Services
Easy reading: To receive this policy/procedure in a different format, please contact HR Services