Information Security and Compliance Policy

Author: The Executive Team Member with Responsibility for Data Protection and GDPR

Approved: 15 October 2024 (Audit Committee)

Review: October 2027

Contents

Introduction

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as the Harlow College where information will relate to learning and teaching, research, administration and management. This policy is concerned with the management and security of the College's Information and the use made of this Information by its members and others who may legitimately process College information.

The Information Security and Compliance Policy is the overarching document of Harlow College's Data Protection Framework and is intended to provide an overview of Information Security best practice. This policy should be read in conjunction with the Frameworks other policies and guidance, some of which fall outside the scope of IT Services.

Purpose

The purpose of this policy is:

- to ensure that all Harlow College Information and Information systems are adequately protected against the adverse effects of failures
- to ensure that users can maintain the confidentiality, integrity and availability of Information used within the College
- to ensure that Harlow College implement the appropriate measures to ensure regulatory, legal and contractual compliance

Scope

This policy applies to anyone using Harlow College IT facilities (hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by Harlow College. The terms of this policy apply in whatever location a user is working (whether or not on our premises).

Policy Statement

Organisation of Information Security

The Deputy Principal has ultimate accountability for implementing Information Security at Harlow College.

The College has appointed an Executive Director to oversee the task of ensuring that all Information and Information systems which are of value to Harlow College are adequately protected against the adverse effects of Information Security breaches. The Executive Director has the authority to assess requests that may have an impact on Information Security and make decisions regarding issues that may adversely affect the College's overall Information Security.

Awareness

All users of Harlow College IT facilities will receive appropriate Information Security awareness training and guidance as part of Data Protection training in relation to successfully conforming to Information Security best practices when carrying out any duties on behalf of Harlow College.

Members of staff are expected to read and comply with the terms outlined within the other policies that make up the wider Data Protection framework. Over time, other policies may be added to this framework. When this occurs affected users may be notified by a variety of means including:

- Training and Workshops
- Email communication
- Desktop notifications
- Intranet announcements

Compliance

Harlow College has established this policy to promote Information Security and Compliance with relevant legislation a full list of which is contained within the Acceptable Use Policy. Harlow College regards any breach of Information Security requirements as a serious matter, which may result in disciplinary action.

Compliance with this policy and relevant supporting policies, practices or procedures should form part of any contract with a third party that may involve access to network or computer systems or data.

All IT services, and products used to operate those services, must be appropriately licenced.

All users must respect the rights of intellectual property, copyright and trademark owners.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist.

Staff

This Information Security and Compliance Policy is part the data protection policy contained in staff terms and conditions of employment issued by Human Resources.

Agreements with third parties involving accessing, processing, communicating or managing the College's Information or Information processing facilities, or adding products or services to Information processing facilities, shall cover all relevant security requirements.

All such agreements will be subject to the satisfactory completion of a Data Sharing Agreement that sets strict guidelines between Harlow College and the approved third party on how that Information will be transferred, used stored, managed and destroyed.

If a member of staff has been found to be in breach of the Information Security and Compliance Policy resulting in an Information Security breach, they may be subjected to the Disciplinary Procedures.

Students

This Information Security and Compliance Policy forms part of the terms and conditions that you accept when you agree to study at Harlow College.

When you use Harlow College IT facilities you are agreeing to be bound by the terms and conditions set out within all of the policies, procedures and guidance outlined within the Data Protection Framework.

If a student has been found to be in breach of the Information Security and Compliance Policy that results in an Information Security breach, they may be subjected to Disciplinary Procedures.

User Account Control

Harlow College uses a user registration and de-registration procedure for granting and revoking access to all Information systems and services.

All users shall have a unique identifier (user ID) for their personal use only; User ID must not be used by anyone else and associated password must not be shared with any other person for any reason.

The allocation of privileges is restricted to ensure that the level of access privilege is limited to what is required for a user to carry out their duties.

Password management is detailed in the Password Protection Guidelines. The allocation of passwords is controlled through a formal management process.

A user's access rights are reviewed at regular intervals, if a staff member or student leaves the College IT Services will disable the users account to restrict unauthorised access as determined by business needs.

Users are required to follow good security practices in the selection and use of passwords as defined in the Password Construction Guidelines.

Third-party accounts are assigned a Harlow College owner. The assigned owner is responsible for ensuring that the account and the user comply with the policy and the account status is reviewed on a periodic basis. Access to third parties should be limited to the minimum period required.

Physical Access Controls

Security perimeters (barriers, card controlled entry gates and doors or manned reception desks) are used to protect areas that contain Information and significant IT equipment.

All equipment and data that is located on College premises is protected from theft, loss or damage using a variety of detective and preventative means.

All visitors to Harlow College are expected to make themselves known to the relevant campus reception area and register their arrival and departure. All visitors are required to wear a visitor's pass and should be accompanied by a member of Harlow College staff at all times.

Network Access Controls

Users of Harlow College IT facilities should only to be provided with access to the services that they have been specifically authorised to use as part of their role or function. Responsibility for ensuring that a user has authority to access a service should be determined by the relevant department.

Access is monitored to identify unauthorised access.

Appropriate security controls have been implemented where the Internet enters the Harlow College network to mitigate known and on-going threats.

Security controls will also be implemented to protect local network segments and the IT resources that are attached to those segments.

Mobile and Remote Access Control

Where remote access is required, this is provided via a defined Remote Access Guidelines to allow the required access necessary.

Appropriate authentication methods are used to control access by remote users.

Security measures have been implemented to protect against the risks of using mobile computing and communication facilities including the requirement for pin protection on all Harlow College devices connecting to the network and accessing email.

Removable Media and Transmission of Data

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations. The management of this risk all users must refer to the Removable Media Guidelines for acceptable use.

Email Use

The use of IT Facilities for Email is governed by the terms set out in the Harlow College Email Policy, the associated Guidance for Staff and Student.

Internet Use

The use of IT Facilities for browsing the Internet is governed by the terms set out in the Acceptable Use Policy.

Internet services are not be used to browse illegal or offensive material. IT Services have measures in place to monitor and log the web traffic of all users, in addition to having the ability to prohibit access to websites and services that are deemed inappropriate for College use.

Social media services must not be used to abuse individuals or groups. Users should refer to acceptable use policy.

A log of activity and the identity of the user will be recorded to permit the resolution of complaints and to investigate abuse.

Incident Management

IT Services maintain an Information Security & Disaster Recovery Plan that relies on ongoing operational monitoring and incident response procedures to be effective. If a user becomes aware of any issue that may impact up on the security of Information Security at Harlow College they are obliged to contact the Helpdesk as soon as possible.

Monitoring

In order to protect Information belonging to the College and the personally identifiable information of its users' the Harlow College monitors and records the use of its IT facilities. Specific purposes for monitoring include:

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct;
- Compliance with lawful requests for Information from government and law enforcement agencies;
- To ensure Harlow College meets statutory duty, under the safeguarding and PREVENT legislation

Users must not attempt to monitor the use of the IT facilities using any technological, or physical means and it is a criminal offence to meaningfully subvert and/or modify data being processed by IT facilities.

Other Relevant Policies/Guidelines

Acceptable Use Policy
Password Construction Guidelines
Password Protection Guidelines
Remote Access Guidelines
Data Protection Policy
Removable Media Guidelines
Bring Your Own Device (BYOD) Policy

Reporting

Any actual or suspected breach of this policy should be reported to IT Services immediately upon discovery. Any device in breach of this policy can be brought to IT Services who will rebuild the device to ensure compliance with the policy.

The Version's Changes

Version	By	Date	Summary
1	Ben Nicholl	September 2024	Document Review. Added Version Control.

TRACKING and REFERENCE INFORMATION
Date Approved: 25 March 2021, 15 October 2024 (Audit Committee)
Review Date: October 2027
Author/Responsibility: Executive Team Member with responsibility for Data Protection and GDPR
Equality Impact Assessment: n/a
List of related policies, procedures and other documents: Acceptable Use Policy Password Construction Guidelines Password Protection Guidelines Remote Access Guidelines Data Protection Policy Removable Media Guidelines Bring Your Own Device (BYOD) Policy
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 Executive Team Member with responsibility for Data Protection and GDPR.
Easy reading: To receive this policy/procedure in a different format, please contact HR Services