Harlow College Data Protection Policy 2018

Policy Owner: Deputy Principal, Mike Stokes
Approved: Corporation (Full Board) 15 March 2018
To be reviewed: March 2021

CONTENTS

1. Introduction

The College needs to keep certain information about employees, students and other users to allow it to monitor for example performance, achievement and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and Government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully.

2. Definitions

Consent any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

DPO	Data Protection Officer
Data Controller	a person, public authority, agency or other body which (either alone or jointly or in common with other persons) determines the process for which and the manner in which any personal data are, or are to be, processed
Data Processor	any person, public authority, agency or other body which processes the data on behalf of the data controller
Data Regulator	the regulator is the Information Commissioners Office
Data Subject	the individual whose data we are processing
Funding Agencies	These are the bodies that we receive funding from to provide education. These include Educations Skills Funding Agency and Higher Education Funding Council for England.
GDPR	General Data Protection Regulations
Personal Data	data which relates to a living individual who can be identified and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special Category Data	personal data relating to the subject’s racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; or any offence, alleged offence or proceedings disposal of such proceedings or the sentence of any court in such proceedings. Additional rules apply in relation to the disclosure of such data.

Subject Access Request	a written, signed request from an individual to the Data Protection Officer to see information held on them.

3. Legal

The College has allocated the responsibility of Data Protection Officer (DPO) to the Deputy Clerk to the Corporation who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

The College recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 and is actively working towards compliance with that directive.

4. Principles

The College shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the GDPR:

Principle 1 Lawfulness, fairness and transparency

Transparency:	Tell the subject what data processing will be done
Fair:	What is processed must match up with how it has been described
Lawful:	Processing must meet the tests described in GDPR [article 5, clause 1(a)]

Principle 2 Purpose limitations

Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Principle 3 Data minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.

Principle 4 Accuracy

Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

Principle 5 Storage limitations

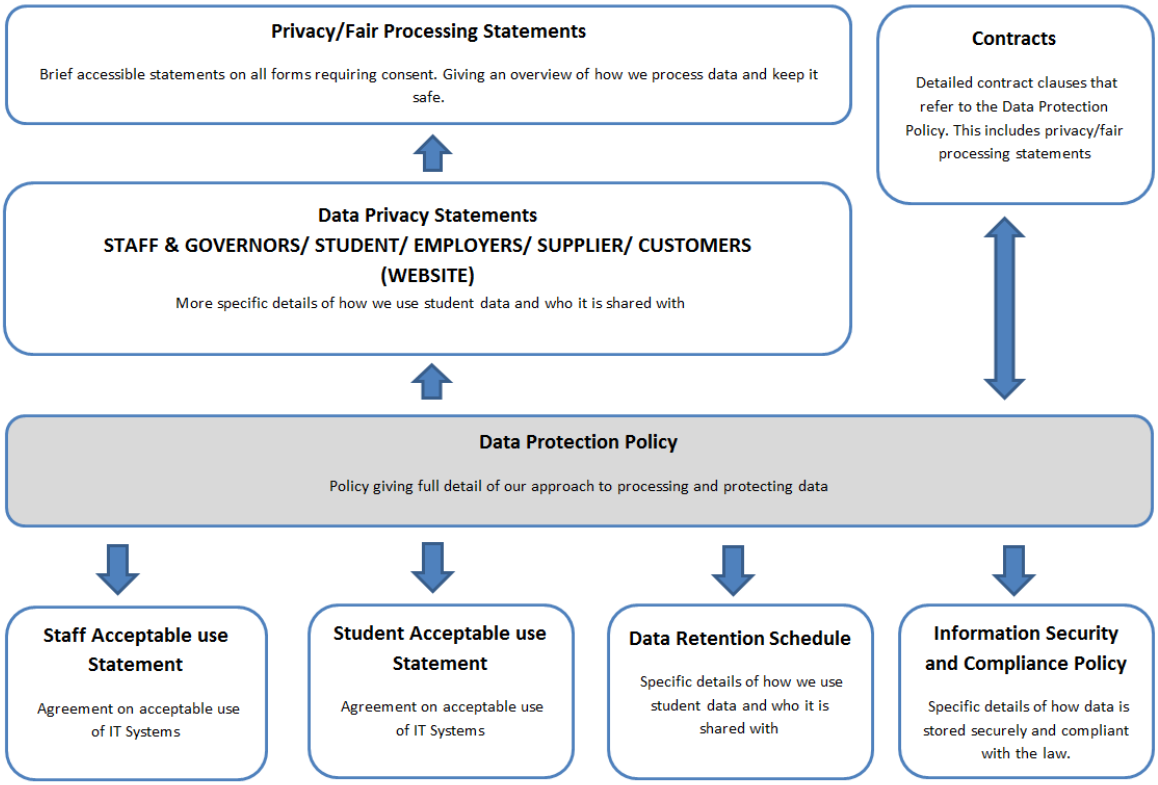
Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.

Principle 6 Integrity and confidentiality

Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage” [article 5, clause 1(f)].

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

5. Working Practice/Principles in Action



Collecting Data

Harlow College will be undertaking an approach to data processes that promotes privacy and data protection compliance from the start (privacy by design). All new processes and systems using data should be designed with privacy in mind and a Privacy Impact Assessment (PIA) carried out where appropriate. PIAs are likely to become compulsory by law in the near future. Please contact DPO for an assessment. More information is available on the ICO website.

In compliance with the GDPR obligations, Harlow College will review on an ongoing basis all personal and special categories of personal data that is collected to ensure that there is a legitimate business reason to justify its collection and processing. When collecting personal and special categories of personal data, the College will conduct informal impact assessments which weigh up those business interests against the interests of the data subject which will be a means of demonstrating a reasoned and balanced approach. On collection of personal and special categories of personal data, the College will ensure that consent is freely given and data subjects have access to our approach to processing, sharing and retaining data.

Processing Data

When processing data the College will ensure one of the (below) lawful bases for processing as set out in Article 6 of the GDPR applies:

(a) Consent:	the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract:	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

We will ensure that it gives employees appropriate instructions regarding how they are to handle personal data on the institution's behalf. This will include:

- if they can share the information and how they do this securely
- processing in line with appropriate consent
- how they store information securely
- how they can respond to questions, concerns or incidents

Data will only be processed in line with its original purpose for collection unless there is a legal basis or further consent is gained. All data subjects will be able to access the information that the College holds on them to ensure its accuracy, to correct their data or to withdraw consent at any time (where consent has been asked for).

Sharing Data with Partners

Personal and/or Special Category data will only be shared with third party organisations where there is a legitimate purpose; data subjects have been informed with the relevant level of consent has been sought. When sharing personal and/or special category data with other organisations we will ensure that this is done by secure means ensuring it can only be accessed by the intended recipient. For organisations that we share personal and/or special category data we will seek assurance that there approach to processing personal and/or special category data is compliant with GDPR.

Retention of data

Harlow College will ensure that the data held will be strictly "limited to the minimum necessary". This will mean that data will only be retained for a period that is necessary for business or legal purposes. For the full details of how long the College will retain data please see our Data Retention Schedule.

Rights of Data Subjects

We are committed to ensuring all data subjects are able to exercise their rights under the regulation and below details how we uphold these rights:

Right to be informed	Privacy statements clearly set out our approach to how and why we process data.
Right of access	All requests to access personal and/or special category data must be made in writing to the Data Protection Officer. These will be responded to within one calendar month.
Right to rectification	All requests in the first instance should be directed to the relevant department, i.e. Central Administration Team for students, Human Resources for staff.
Right to erasure	All requests to erase personal and/or special category data must be made in writing to the Data Protection Officer. These will be responded to within one calendar month.
Right to restrict processing	All requests in the first instance should be directed to the relevant department, i.e. Central Administration Team for students, Human Resources for staff.
Right to data portability	All requests data portability must be made in writing to the Data Protection Officer. These will be responded to within one calendar month.
Right to object	In the College's data collection processes and communications with data subjects, we will ensure it is clear how to exercise their right to object. All requests in the first instance should be directed to the relevant department, i.e. Central Administration Team for students, Human Resources for staff.

Rights in relation to automated processing and profiling – This is not applicable to Harlow College

6. Roles & Responsibilities

All staff:

All staff are responsible for ensuring that:

- any personal data which they hold is kept securely; and
- personal information is not disclosed to any unauthorised third party (orally, in writing or electronically).

Staff should note that unauthorised disclosure will usually be a disciplinary matter.

When not in use, personal information should normally be:

- kept in a locked filing cabinet /drawer; or
- if it is computerised either be password protected or kept only on a storage device which is encrypted and kept securely. Encrypted memory sticks please contact IT Helpdesk.

In respect of their own personal data, staff have a responsibility to;

- ensure that any information they provide to the College in connection with their employment is accurate and up to date; and
- inform the College of any changes to information that they have provided, e.g. change of address.

In respect of all other personal data that they hold, process or have access to in connection with their employment they are responsible for ensuring that they comply with these procedures and follow the published guidance on QUBE (this link is only accessible to staff).

All Students

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that any changes in personal details such as change of address are notified to the appropriate person - normally their tutor. They must also comply with the College's Acceptable Use Statement.

Designated Data Protection Officer

The College as a corporate body is the data controller under the Regulation, and the Board of Governors is therefore ultimately responsible for implementation. However, the designated Data Protection Officer who is appointed to ensure compliance with the Regulation is:

- Deputy Clerk to the Corporation

and appointed to deal with day-to-day matters to ensure processes are robust and in line with the legislative requirements:

Other senior managers responsible for ensuring compliance with GDPR are as follows:

• Executive Director – Information, Data and Support	Learner Records
• Executive Director – Human Resources	Employment Records
• Executive Director – IT, Facilities and Exams	IT Infrastructure and Security
• Executive Director – Financial Services	Financial Records
• Assistant Principal – Student Services	Safeguarding and Child Protection
• Assistant Principal - Apprenticeships	Employer Records
• Clerk to the Corporation	Governor Records

7. Monitoring

As part of the ongoing monitoring there will be Data Protection Monitoring and GDPR compliance that will be cross-cutting across all internal audits to ensure that practice is in line with guidance. This will be further supported by regular training to ensure teams are compliant with this and related policies.

The DPO will meet with members of the Executive team on a regular basis to ensure staff are receiving the right training, update policy, review working practices and monitor the compliance across the organisation.

8. Enforcements & Breaches

Any loss of data must be reported to the Data Protection Officer (DPO) for an assessment of the risks associated with the breach.

In addition, if special or personal data about a student or member of staff is either inadvertently released or used inappropriately, the DPO is to be informed as soon as the breach is discovered so that appropriate action can be taken.

The DPO is responsible for:

- informing appropriate people and organisations that the breach has occurred;
- notifying serious breaches (based on current ICO guidance);
- implementing a recovery plan, including damage limitation; and
- reviewing and updating information security.

9. Linked policies, procedures and guidance

For further information and guidance, please see……

- Student Acceptable use Statement
- Staff Acceptable use Statement
- Data Privacy Statements
- Data Retention Schedule
- Information Security and Compliance Policy

To find out more about the General Data Protection Regulation please visit www.ico.org.uk

TRACKING and REFERENCE INFORMATION	
Date Approved:	**15 March 2018**
Review Date:	**March 2021**
Author/Responsibility:	**Deputy Principal**
Equality Impact Assessment: n/a	
List of related policies, procedures and other documents: All Harlow College Policies, guidelines and briefings	
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 the Designated Data Protection Officer (Deputy Clerk)	
Easy reading: To receive this policy/procedure in a different format, please contact HR Services.	