Data Protection Policy

This policy sets out a framework for dealing with data. The policy is applicable to all employees within the Plumpton College Group. For the avoidance of doubt the policy is non contractual.

Any reference to Plumpton College is relevant to the Plumpton College Group, meaning any employee employed by its subsidiaries, its holding company or any subsidiary of its holding company.

SMT Assigned Owner	Deputy Principal
Document Author	Deputy Principal
Approved by	Corporation
Date of Approval	22nd February 2022
Date of minor amendments approved by SMT	-
Frequency of review	3 years
Date of next review	February 2025

The SMT is delegated to approve minor changes to the policy in response to legal changes and best practice.

Table of Contents

INTRODUCTION 2
DEFINITIONS 3
COLLEGE RESPONSIBILITIES 4
RIGHTS OF THE INDIVIDUAL (DATA SUBJECT) 5
LAWFULNESS OF PROCESSING 6
1. *Consent* 6
2. *Performance of a Contract* 6
3. *Legal Obligation* 7
5. *Task Carried Out in the Public Interest* 7
6. *Legitimate Interests* 7
PRIVACY BY DESIGN 7
CONTRACTS INVOLVING THE PROCESSING OF PERSONAL DATA 8
BREACHES OF PERSONAL DATA 8

Introduction

In its everyday operations, Plumpton College (the College) makes use of a wide range of personal data about identifiable individuals including:

- Current, past and prospective students
- Employees and Governors
- Users of its websites and online shops
- Other stakeholders (for example – visitors, employers, suppliers, parents)

In collecting and using this data, the organisation is subject to legislation, in particular the UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018.

The EU GDPR remains part of UK law following the Brexit transition period given that UK companies process the personal data of EU citizens and as such it defines how how such data use may be carried out and the safeguards that must be put in place to protect it. For the purpose of clarity within the college, both the UK and EU GDPR are aligned in how the college is expected to process personal data. As such, our compliance against the UK GDPR can be interpreted as compliance against the EU GDPR.

The College is accountable to the *Information Commissioner (www.ico.org.uk) as* the supervising authority for all matters regarding information rights. Fines of up to 4% of gross turnover are applicable if a data breach is deemed to have occurred under the GDPR. Such a fine would have a significant impact upon the College's operations and as such the protection, confidentiality and integrity of personal data is a key responsibility of everyone within the College.

The purpose of this policy is to set out the basis by which the College will comply with the relevant legislation. This control applies to all systems, people and processes that constitute the College's information infrastructure. It is therefore an underpinning requirement of the working culture that the College requires from all employees and is as applicable to the security of information within offices and classrooms as it is to that held online.

The following policies and procedures are in place to allow staff to interpret and act in accordance with this policy.

- *IT Security Policy*
- *Data Review Procedure*
- *Information Security Incident Response Procedure*

- *Records Retention and Protection Policy*

Definitions

There are a number of definitions listed within the UK GDPR and it is not appropriate toreproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal Data is defined as any information relating to a living person ('data subject') which allows them to be identified directly or indirectly. Such information can take any form and can include (list is not exhaustive):

- factual information (date of birth, contact details, gender)
- opinions based upon that person's actions or behaviours
- image, video and audio files
- online identifiers and financial information

Sensitive Personal Data includes information such as a data subject's ethnic origin, health data, religion, sexual orientation and biometric information. This is a subset of personal data and requires a greater level of protection.

Processing means any operation which is performed on personal data, whether or not by automated means, such as collection, recording, storage, adaptation or alteration, retrieval, disclosure by transmission, erasure or destruction.

Data Controller means any entity (such as an organisation, company or authority) that decides how it will process personal data. The College is the Data Controller.

Data Breach can apply to a range of scenarios. Examples within the context of the College could include but are not limited to:

- using the image of an identifiable person without their consent
- allowing the recipient of an email to see the personal email addresses of other recipients
- leaving hard copies of personal data unsecured in offices and classrooms
- storing data on staff and students in shared folders without password protection or an agreed permissions structure
- through a case of mistaken identity discussing the personal circumstances of a student with another.

College Responsibilities

As a Data Controller the College has a duty to uphold the following privacy principles and will ensure that personal data is:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject. The lawful basis adopted by the College will be clarified in the relevant privacy notice.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) adequate, relevant and limited to the minimum that is deemed necessary in relation to the purposes for which they are processed

(d) accurate and, where necessary, kept up to date

(e) kept in a form which permits identification of data subjects for no longer than is necessary

(f) 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

The Principal has overall responsibility for legislative compliance and delegates this duty to the Deputy Principal as Data Protection Officer. The College has also appointed a Data Subject Access Request Administrator.

System Leads are identified within college managers to work closely with the IT Team and to act as a point of contact, a point of administration, to participate in system update testing and to provide an ongoing appraisal of the functionality, interface and impact of a particular system on college operations. The main systems are as follows:

System Leads	System
Director of Finance	Unit 4 – Agresso Albany E-Pay Online Shop

Student Records Manager	Pro Solution Pro Achieve Pro General Funding Information Suite

MIS Director	Pro Solution Pro Achieve Pro General Funding Information Suite 4Cast Provider Data Self-Assessment Toolkit
Director of Quality	Pro Monitor Pro Portal
HR Manager	Midland HR
Head of Marketing, Communications and Customer Experience	Akero (or another if replaced) Staff Intranet
IT Ops Manager	Main Data Centre Network infrastructure Microsoft Exchange Online
Student Services Manager	Net2 Access Control CCTV
Estates Manager	CAFM Archive file storage arrangements
Library	Heritage LMS
Health & Safety Manager	Accident reporting system

All staff are responsible for supplying and maintaining accurate personal data and for complying with the data processing principles set out above and key security actions as part of their core accountabilities.[1]

Rights of the Individual (Data Subject)

The data subject's rights are clarified within the UK GDPR. The College upholdsthese rights by:

1. The right to be informed – this is achieved through privacy notices
2. The right of access – this will be provided to the data subject within one month and will usually be provided free of charge.
3. The right to rectification – this will be undertaken within one month.

[1] Aspects of which are further clarified in the IT Security Policy.

4. The right to erasure – this will be undertaken without undue delay subject to the College continuing to meet its legal obligations concerning personal data retention.
5. The right to restrict processing – this will be undertaken without undue delay subject to the College continuing to meet its legal and contractual obligations which rely on certain processing activities.
6. The right to data portability – this will be undertaken within one month and data will be provided to the data subject or a nominated controller in a useable and acceptable format.
7. The right to object – the College will stop any processing activity related to direct marketing upon receipt of an objection. The College will engage with the data subject to reach an agreement within the law and without undue delay for other objections.
8. Rights in relation to automated decision making and profiling – the College will ensure that privacy notices accurately convey any automated processing and profiling activities.

Lawfulness of Processing

There are six alternative ways in which the lawful processing of personal data may be established under the UK GDPR. System Managers will identify the appropriate basis forprocessing and the Data Protection Officer will audit such decisions through the Data Review Procedure.

1. Consent

Unless it is necessary for a reason allowable in the UK GDPR, the College will always obtain explicit and positive consent from a data subject to collect and process theirdata. In case of children below the age of 16 parental consent will be obtained.
Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent.

2. Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question. For example; an initial assessment on a student cannot be undertaken without qualification and assessment data.

3. Legal Obligation

If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. For example, this may be the case for some HR data related to employment and taxation or to government funding organisations.

4. Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basisof the processing. Such examples would ordinarily fall under the remit of the College's safeguarding policy where the College may need to contact an external agency about a student in order to ensure their safety.

5. Task Carried Out in the Public Interest

Where the College needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. This basis is unlikely to apply to the College and is more relevant to local authorities. Employees should not process data on this basis without authority from the Data Protection Officer.

6. Legitimate Interests

If the processing of specific personal data is in the legitimate interests of the College and is judged to be of relevance and mutual interest whilst not affecting the rights and freedoms of the data subject in a significant way, then this may be defined as thelawful reason for the processing. For example; marketing information about vocationally specific short courses would be sent to previous students studying similar courses on this basis. Such activity would seek to establish consent following first contact.

Privacy by Design

The College has adopted the principle of privacy by design and will ensure that the definition and planning of all new projects[2] will be subject to due consideration of privacy issues, including the completion of Data Review exercises.

The Data Review exercise as a minimum will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation
- What further measures could be adopted to further enhance data security.
- What privacy notices need to be updated/created.

The Data Review process will be undertaken annually as a minimum by System Managers.

Contracts Involving the Processing of Personal Data

The College will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that clearly identifies the Data Controller, the Data Processor and what processing actions are permitted within the contract.

Breaches of personal data

All incidences of loss, theft or unauthorised disclosure of personal data must be reported as soon as possible to the Data Protection Officer.

It is the College's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the UK GDPR, where a breach is known to have occurred which is likely to result in a riskto the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our *InformationSecurity Incident Response Procedure* which sets out the overall process of handling information security incidents.

[2] Such projects are not limited to the development of new online systems. The considerations required are equally applicable when planning new office moves or accommodation.

Addressing compliance to the UK GDPR

Compliance with the UK GDPR is the responsibility of all members of the College and any deliberate, reckless or negligent breach of this policy may result in disciplinaryaction.

End of Policy