



Data Protection & GDPR Policy

Reviewed:	September 2023
To be reviewed:	September 2024
Version	7

NAME OF 1st REVIEWER	Emily Hollis
NAME OF 2nd REVIEWER	Lauren Lawley

Contents

Introduction	2
Aims	3
Responsibility for the Policy and Procedure.....	3
Role of the Head of College	4
Role of the Data Protection Officer	6
Role of College Personnel.....	6
Role of Parents/Carers	7
Raising Awareness of this Policy	7
Training.....	7
Equality Impact Assessment	7
Monitoring the Implementation and Effectiveness of the Policy.....	8

Introduction

We believe this policy should be a working document that is fit for purpose, represents the college ethos, enables consistency and quality across the college.

We are aware that the General Data Protection Regulations (GDPR) will entirely replace the Data Protection Act (DPA) by making radical changes to many existing data protection rules and regulations that colleges, academies and other educational establishments adhere to under the DPA. The principal aim of the GDPR is to strengthen and unify the safety and security of all data held within an organisation.

We have the duty to ensure that we comply with this new regulation by considering the impact that the GDPR will have on this college and to ensure new policies and procedures are in place before the GDPR comes into effect.

We believe that we comply with the DPA and we realise that many of the GDPR's main concepts and principles are much the same as those in the DPA but we are aware that there are new elements, significant improvements and a new accountability that we need to address. We understand that under the GDPR:

- data management is strengthened and unified
- it will become illegal not to have a formal contract or service level agreement with a chosen data processor
- the data processor must be GDPR compliant
- there will be higher penalties for non-compliance with the GDPR
- data breaches must be reported within 72 hours
- individuals have greater control over their personal data

We are committed to the protection of all personal and sensitive data for which we hold responsibility as the Data Controller. We believe the handling of such data is in line with the data protection principles and that access to such data does not breach the rights of the individuals to who it relates.

We acknowledge the GDPR's definition of personal data as 'meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier' such as name, identification number, location data or online identifier. It applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

The GDPR refers to sensitive personal data as "special categories of personal data" which includes genetic data, and biometric data where such data is processed to uniquely identify an individual by using fingerprints, face recognition or eye screening.

At all times we ensure the principles of the DPA are applied and that all data is:

- processed lawfully
- obtained and processed for specific and lawful purposes
- sufficient, appropriate and not excessive in relation to the precise purpose
- accurate and up to date
- not kept for a great length of time
- processed in agreement with the individual's legal rights
- protected against unlawful processing, accidental loss, destruction or damage
- not to be transferred outside the EU unless the rights and freedom of the individual is protected

We have the responsibility to ensure that all changes to data protection legislation will be monitored and implemented in order to remain compliant with all requirements. All college personnel will attend training in order to be made aware of data protection policies and legal requirements. All contracted service providers will also be notified of our data protection policies and legal requirements.

In preparation for full compliance with the General Data Protection Regulation we have used the 12-step guidance from the Information Commissioner's Office (ICO) in order to identify what changes we need to make.

On completion of the ICO guidance an updated data protection system that fits the needs of the college and complies with the new General Data Protection Regulations will be implemented.

All our data processing activities will be registered with the ICO. The ICO will be notified of any changes to the type of data processing activities being undertaken and the register will be amended accordingly.

We are aware that the GDPR places greater emphasis on accountability and therefore the Data Protection Officer will keep up to date documentation of all data protection activities.

We all have a responsibility to ensure equality permeates into all aspects of college life and that everyone is treated equally irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. We want everyone connected with this college to feel safe, secure, valued and of equal worth.

We acknowledge the findings of the Race Disparity Audit that clearly shows how people of different ethnicities are treated across the public services of health, education, employment and the criminal justice system.

The educational section of the audit that covers: differences by region; attainment and economic disadvantage; exclusions and abuse; and destinations, has a significant importance for the strategic planning of this college.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Aims

- To ensure compliance with the General Data Protection Regulations
- To strengthen and unify the safety and security of all data held within the college
- To ensure the protection of all personal and sensitive data for which we hold responsibility as the Data Controller
- To ensure the handling of all personal and sensitive data is in line with the data protection principles
- To undertake an audit of the college's current position in preparation for the full implementation of and compliance with the GDPR
- To work with other colleges and the local authority to share good practice in order to improve this policy

Responsibility for the Policy and Procedure

Role of the Head of College

The Head of College have:

- the responsibility to comply with the legal requirements of General Data Protection Regulation 2018;
 - in accordance with the GDPR appointed a Data Protection Officer who has knowledge of data protection law and practices;
 - the responsibility to ensure the DPO:
 - operates independently and is not dismissed or penalised for undertaking their role;
 - keeps the Senior Leadership Team up to date with all data protection activities;
 - has adequate resources to meet their GDPR obligations;
 - keeps up to date documentation of all data protection activities.
 - the responsibility to ensure data is processed in accordance with the eight principles of the Data Protection Act 1998;
 - delegated powers and responsibilities as 'Data Controller' for the college;
 - delegated powers and responsibilities to the Senior Leadership Team to prepare for compliance with the GDPR by following the 12-step guidance from the Information Commissioner's Office in order to identify what changes that we need to make to the current data protection system;
 - delegated powers and responsibilities to the Senior Leadership Team that on completion of the guidance to devise and implement an updated data protection system that fits the needs of the college and complies with the new GDPR;
 - delegated powers and responsibilities to ensure all college personnel and stakeholders are aware of and comply with this policy;
 - responsibility for ensuring that the college complies with all equalities legislation;
 - responsibility for ensuring funding is in place to support this policy;
 - responsibility for ensuring this policy and all policies are maintained and updated regularly;
 - responsibility for ensuring all policies are made available to parents;
 - responsibility for the effective implementation, monitoring and evaluation of this policy.
 - act as 'Data Controller' for the college;
 - prepare for the General Data Protection Regulation by following the 12-step plan in accordance with the advice from the Information Commissioner's Office:
- **Awareness**
 - To organise awareness training in order to inform all college personnel:
 - that data law is changing to GDPR;
 - to appreciate the impact, it will have on the college;
 - how the impact will affect the college;
 - by identifying areas that could cause compliance problems under the GDPR.
 - To hold refresher training for all college personnel when necessary.
 - **Information we hold**
 - To organise an information audit of data held on learners, college personnel, parents and suppliers.
 - The audit will be undertaken under the following headings:
 - The type of data.
 - How is the data collected?
 - How is it processed?
 - Where did it come from?
 - Where is it located?
 - How is it secured?
 - Who is it shared with?

- **Communicating Privacy Information**
 - To review current privacy notices and to undertake any necessary changes before the implementation of GDPR.
- **Individuals' Rights**
 - To check current procedures to ensure they cover all the rights of individuals have including:
 - how to delete personal data; and
 - how to provide data electronically in a commonly used format.
- **Subject Access Requests**
 - To update present procedures and to plan how to handle requests within the new one-month timescale and to provide any additional information.
- **Legal basis for protecting personal data**
 - To review the various types of data processing that the college carries out and then identify and document the legal basis for carrying it out.
- **Consent**
 - To review how the college seeks, obtains and records consent and consider any changes that are required.
- **Learners**
 - To 'start thinking now about whether we need to put systems in place to verify individuals ages and to obtain parental or guardian consent for any data processing activity.'
- **Data breaches**
 - To ensure the right procedures are in place to detect, report and investigate a personal data breach.
- **Data protection by design and data protection impact assessments**
 - To consider when to begin implementation of the Privacy Impact Assessments.
- **Data Protection Officers**
 - To have in place a designated Data Protection Officer to take responsibility for data protection compliance.
 - To assess where this role sits within the college's structure
- **International**
 - To determine (if the college operates internationally) under which data protection supervisory authority applies to the college.
- keep a detailed record of all activities while undertaking the 12-point plan;
- ensure the college complies with the GDPR;
- works closely with the Data Protection Officer and the Senior Leadership Team;
- ensure the college complies with the eight data protection principles;
- ensure all data is processed fairly and lawfully;
- ensure security measures and confidential systems are in place to protect personal data and learner records;
- ensure data is obtained for specific and lawful purposes;
- ensure data is adequate, relevant and not excessive;
- ensure all personal data is accurate and that inaccurate data is corrected or erased;
- ensure that at the beginning of every academic year all college personnel will receive a copy of their personal data;

- ensure procedures are in place to deal with requests for access to personal data;
- ensure data is not kept longer than is necessary;
- ensure college personnel are aware of their rights;
- ensure college personnel are aware of their responsibilities;
- ensure a learner's educational records will be made available to their parents or carers on receipt of a written request;
- make effective use of relevant research and information to improve this policy;
- provide leadership and vision in respect of equality;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy by speaking with learners, college personnel and parents.

Role of the Data Protection Officer

The Data Protection Officer will:

- have expert knowledge of data protection law and practices;
- inform the college and college personnel about their obligations to comply with the GDPR and other data protection laws;
- ensure data management is strengthened and unified;
- monitor compliance with the GDPR and other data protection laws;
- manage internal data protection activities;
- ensure risk and impact assessments are conducted in accordance with ICO guidance;
- report data breaches within 72 hours;
- ensure individuals have greater control over their personal data;
- ensure that prior to the processing of an individual's data that:
 - the process is in line with ICO guidance;
 - the process is transparent;
 - the individual will be notified;
 - the notification is written in a form that is understandable to learners;
 - when sharing an individual's data to a third party outside of college that details for the sharing are clearly defined within the notifications.
- share an individual's data where it is a legal requirement to provide such information;
- process all written subject access requests from individuals within 40 days of receiving them;
- have in place a formal contract or service level agreement with a chosen data processor who is GDPR compliant;
- ensure the secure disposal of redundant data and IT hardware holding data in compliance with ICO guidance;
- train college personnel;
- conduct audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed;
- keep up to date documentation of all data protection activities.
- work closely with the Directors and Senior Leadership Team;
- periodically report to the Directors and Senior Leadership Team;
- report to the Directors on the success and development of this policy.

Role of College Personnel

College personnel will:

- attend GDPR awareness training.
- comply with all aspects of this policy.
- be aware of all other linked policies.

Role of Parents/Carers

Parents/carers will:

- be invited to attend GDPR awareness training.
- comply with all aspects of this policy.
- be aware of all other linked policies.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the College Handbook/Prospectus.
- the college website.
- the Staff Handbook.
- meetings with college personnel.
- communications with home such as weekly newsletters and of end of half term newsletters.
- uploading to the CPOMS Library for ease of reference.

Training

All college personnel:

- have equal chances of training, career development and promotion
- receive training on this policy which specifically covers:
 - General Data Protection Regulation
 - Data Protection Act 1998
 - Freedom of Information 2000
 - Access to Personal Records
 - E-safety
 - Grievance Procedure
 - Equality
- receive periodic training so that they are kept up to date with new information
- receive equal opportunities training on induction in order to improve their understanding of the Equality Act 2010 and its implications

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any learner and it helps to promote equality at this college.

Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the Head of College and Senior Leadership Team.