**Contents**

1. Overview ..... 3
2. About the policy ..... 3
3. Definitions ..... 3
4. College Personnel's General Obligations ..... 5
5. Data Protection Principles ..... 5
6. Lawful Use of Personal Data ..... 6
7. Transparent Processing – Privacy Notices ..... 6
8. Data Quality – Ensuring the Use of Accurate, Up to Date, Relevant Personal Data ..... 7
9. Data Retention ..... 7
10. Data Security ..... 8
11. Data Breach ..... 8
12. Appointing Contractors Who Access the College's Personal Data ..... 8
13. College Personal's Obligations Regarding Data Requests ..... 9
14. Individual's Rights ..... 10
15. Marketing and Consent ..... 12
16. Automated Decision Making and Profiling ..... 12
17. Data Protection Impact Assessments (DPIA) ..... 13
18. Transferring Personal Data to a Country Outside the UK ..... 14

| | |
|---|---|
| **Programme / Business Area:** | Information & Technical Services |
| **Prepared By:** | Assistant Principal Curriculum Development, Information & Technical Services |
| **Next Review Date:** | November 2024 |

## 1. Overview

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores Personal Data relating to individuals and organisations including employees, students, suppliers, visitors and others. The College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws.

The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of personal data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

College staff will be signposted to a copy of this Policy when they start and may receive notifications of revisions. This Policy does not form part of any member of the College personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

## 2. About the policy

This Policy (and the other policies and documents referred to in it) set out the basis on which the College will collect and use Personal Data either where the College collects it from individuals directly, or where it is provided to the College by third parties. It also sets out rules on how the College handles, uses, transfers and stores personal data.

It applies to all personal data stored electronically, in paper form, or otherwise.

The legal responsibility for compliance with Data Protection Law lies with the College who is the 'data controller', registered as such with the Information Commissioner's Office. Responsibility for compliance is delegated to College Managers who are responsible for encouraging data processing best practice within the College. However, compliance with this policy is the responsibility of everyone within the College who processes personal information.

## 3. Definitions

**College Personnel –** Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College**.**

**Controller –** Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the

Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

**Data Protection Laws** – The Data Protection Act 2018 sets out the framework for data protection law in the UK. It came into effect on 25 May 2018 and was subsequently amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR which is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context. Where any overseas data was collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. This gives people specific privacy rights in relation to electronic communications.

**Data Protection Officer** – The College

- x kept for no longer than is necessary for the purposes for which it is being processed;
- x 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.

These principles are considered in more detail in the remainder of this Policy.

In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

## 6. Lawful Use of Personal Data

In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. These are documented in the Data Use and Retention Schedule

In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Where possible we will try to obtain your explicit consent, unless it is a requirement of our statutory duty.

The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

## 7. Transparent Processing – Privacy Notices

Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy

BOLTON C (O)- 9.96 -0o984T364 804.24 7EG04.1364 E D9.96 -0A2 (19.5-0A (11.7O)-PR9.96 -0o984)-22 (N)5-0E 9.96 -0

## 10. Data Security

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

## 11. Data Breach

Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

There are three main types of Personal Data breach which are as follows:

**Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information

Any contract where an organisation appoints a Processor must be in writing.

You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

UK GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of UK Data Protection Law.

In addition the contract should set out:

- The subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

## 13. College Personal's Obligations Regarding Data Requests

This Policy sets out the rights that individuals have over their Personal Data under Data Protection Laws. If a member of the College Personnel receives a request from an individual to exercise any of the rights set out in this Policy, that member of the College Personnel must:

- inform the Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request;
- tell the Data Protection Officer what the request consists of, who has sent the request and provide the Data Protection Officer with a copy of the request;
- not make any attempt to deal with, or respond to,.6 (er)-6 2 (,)4.3 ( ) (t)-6.6a P(o)10. ( w)2.6 (i)2.6 (t)

## 14. Individual's Rights

### Subject Access Requests

Individuals have the right under the UK GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). In addition, the College is no longer able to charge a fee for complying with the re Td(I)Tj-.04 -0 0 8.04 .9 0 8.04 .9 0

When an individual asks the College to delete their Personal Data, the College is required to do so and to inform the individual in writing within one month of them making the request that this has been done.

**Right of Data Portability**

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means

This right isn't the same as subject access and is intended to give individuals a subset of their data. This right is to obtain from the College a copy of their own Personal Data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as its legitimate interests.

The College is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that the College explains to the individual why it needs more time).

The individual also has the right to ask the College to transmit the Personal data directly to another organisation if this is technically possible. Such requests must be in writing.

**The Right of Rectification and Restriction**

Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

Individuals have the right to ask the College to correct any Personal Data about them that the College is holding that is incorrect. The College is then obliged to correct that Personal Data within one month (or two months if the request is complex).

Where the individual tells the College their Personal Data is incomplete, the College is obliged to complete it if the individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

If the College has disclosed the individual's inaccurate Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction where the College can.

When an individual asks the College to correct their Personal Data, the College is required to do so and to confirm this in writing to the individual within one month of them making the request.

## 15. Marketing and Consent

The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws gthe

**Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

All DPIAs must be reviewed and approved by the Data Protection Officer.

## 18. Transferring Personal Data to a Country Outside the UK

Individuals risk losing the protection of the UK data protection laws if their personal data is transferred outside of the UK. On that basis, the UK GDPR restricts transfers of personal data to a separate organisation located outside of the UK, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

Following the UK leaving the EU, there remains provision that permits the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision'. This is to be kept under review by the UK Government.

Transfer includes sending Personal Data outside the UK but also includes storage of Personal Data or access to it oo(or)-6 ( ( ua[i)2.6 ()2.6 (t(i)2.ns) (,)4.27des)a4 Tw [1 )0.5 ( (m)-6 5)4.27dK4 ( )]TJ-0.01