Bury College Policy and Procedures

Data Protection Policy

Document Information	
Directorate:	Finance and Corporate Services
Document Owner:	Oliver Mackenzie
Document Type	Policy
Date:	October 2022
Version:	1.2
Review Period:	2 years
Date Approved:	01/11/2022
Approved by:	Leadership Team

Version Control Tracking

Version	Date	Revision Description	Editor	Status
V1.0	April 2021	No Revisions	M Doherty	-
V1.1	Sept 2021	Removed privacy, replace with SCC	M Doherty	-
V1.2	Nov 2022	Updated language following UK departure for EU, added paragraph about AADC	O Mackenzie	Active

Bury College
Data Protection Policy
Date: October 2022
Review Date: October 2024

Contents

1. Overview

Bury 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 about its employees, suppliers, sole traders, partnerships or individuals within companies, students, governors, visitors, parents and employers, the College recognises that having controls around the collection, use, retention and destruction of personal data is important to ensure compliance with the College's obligations under Data Protection Laws, in particular, Article 5 of GDPR.

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 personnel will be required to sign a Privacy Notice when they begin with the College and part of that will be agreeing to the principles set out within this policy. 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, at dpo@burycollege.ac.uk, who is responsible for ensuring the College's compliance.

2. About this Policy

This policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use personal data either where the College collects it from individuals themselves, 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.

3. Definitions

3.1. **Age Appropriate Design Code –** The Age Appropriate Design Code (Children's Code/AADC) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. The College will aim to abide by the code where relevant.

3.2. **College** – Bury College

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

3.4. **Controller** – Any entity (e.g. company, organisation or person) which makes its own decisions about how it is going to collect, process, and retain personal data.

A Controller is responsible for compliance with Data Protection Laws. Examples of personal data where the College is the Controller 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.

3.5. **Criminal Offence Data –** Personal data relating to criminal convictions and offences or related security measures. The college requires an authorising condition in Schedule one of the Data Protection Act 2018 alongside a lawful basis to process data of this nature.

3.6. **Data Protection Laws** – The UK General Data Protection Regulation and all applicable laws relating to the collection and use of personal data, privacy, and any applicable codes of practice issued by the regulator, Specific codes of practice for the processing of personal data within the education sector, the age appropriate design code, and the Data Protection Act 2018.

3.7. **Data Protection Officer –** The College's Data Protection Officer can be contacted at: dpo@burycollege.ac.uk.

3.8. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania,Slovakia, Slovenia, Spain, and Sweden..

3.9. **Nations with data adequacy -** Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom and Uruguay

3.10. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

3.11. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

3.12. **Joint Controller** – Joint Controllers are two or more parties that together decide the purposes and/or means of how personal data is used. Bury College will have a Data Sharing Agreement with any organisation with is a joint controller for personal data.

3.13. **Personal data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data (known as special category data) such as trade union membership, genetic data and religious beliefs. Special Category data is given extra protection by Data Protection Laws.

3.14. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal data on the instruction of a Controller.

A Processor is a third party that processes Personal data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involves access to or use of Personal data. They are sperate from Joint Controllers as they are not able to decided how the data is retained. Examples include: where software support for a system, which contains Personal data, is provided by someone outside the business; cloud arrangements etc.

3.15. **Special Category data** – Personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e.

information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation. Special Categories of Personal data are subject to additional controls in comparison to ordinary Personal data.

4. College Personnel's General Obligations

4.1 All College Personnel must comply with this policy.

4.2 College Personnel must ensure that they keep confidential and secure all Personal data that they collect, store, use and come into contact with during the performance of their duties.

4.3 College Personnel must not release or disclose any Personal data:

4.3.1 outside the College; or

4.3.2 inside the college to College Personnel not authorised to access the Personal data,

4.3.3 without specific authorisation from their manager or the Data Protection Officer; this includes verbally or in writing.

4.4 College Personnel must take all steps to ensure there is no unauthorised access to Personal data whether by other member of staff who is not authorised to see such Personal data or by people outside the College.

5. Data Protection Principles

5.1 When using Personal data, Data Protection Laws require that the College complies with the following principles. These principles require Personal data to be:

5.1.1 processed lawfully, fairly and in a transparent manner;

5.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ("Purpose Limitation").

5.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed; ("Data Minimisation").

5.1.4 accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal data that is inaccurate is erased or rectified as soon as possible; ("Accuracy").

5.1.5 kept for no longer than is necessary for the purposes for which it is being processed; and ("Storage Limitation").

5.1.6 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. ("Integrity and Confidentiality").

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

5.3 In addition to complying with the above requirements the College must also 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. (Accountability")

Lawful use of personal Data

5.4 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 lawful grounds.

These are set out in Article 6 of the GDPR and are summarised as follows:

- the processing is necessary for the performance of a **contract**;
- the processing is necessary for compliance with a **legal obligation**;
- the processing is necessary in order to protect the **vital interests** of the individual or of another natural person;
- the processing is necessary for the performance of a task carried out in the **public interest**; and
- the individual who is the subject of the Personal data has given **consent** for one or more specific purposes.

More information about Lawful Basis can be found on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

Lawful purposes for Special Categories of Personal data

5.5 There are additional conditions which need to be met in order to use Special Categories of Personal data. These are set out in Article 9 and include, but are not limited to;

- explicit consent;
- employment and social security obligations;
- vital interests;
- necessary for establishment or defence of legal claims;
- substantial public interest; and
- various scientific and medical issues (including occupational health).

The College will ensure that for each type of Special Categories of Personal data it processes, it has established one of the above legal bases for processing it.

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. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

The College has carefully assessed how it uses Personal data and how it complies with the obligations set out in this policy and will assess these obligations on an ongoing basis. If the College changes how it uses Personal data, the College will update this record and may also need to notify Individuals about the change. If College Personnel, 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.

Criminal Offence Data

5.6 There are additional conditions which need to be met in order to use Criminal Offence data . These are set out in Schedule 1 of the Data Protection Act 2018. These include, but are not limited to.

- Employment, social security and social protection
- Health or social care purposes
- Public health

- Research

The College will ensure that for every instance of law enforcement processing, it has established one of the above legal bases for processing it.

If the College changes how it uses criminal offence data, the College will update this record and may also need to notify Individuals about the change. If College Personnel 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.

6. Transparent Processing – Privacy Notices

6.1 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. Some of the College's Privacy Notices can be seen by following this link www.burycollege.ac.uk

6.2 If the College receives Personal data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal data. This will be provided as soon as reasonably possible.

6.3 If the College changes how it uses Personal data, the College may need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal data please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7. Data Quality – Ensuring the use of accurate, up to date and relevant personal data

7.1 Data Protection Laws require that the College only collects and processes Personal data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice and as set out in the College's record of how it uses Personal data. The College is also required to ensure that the Personal data the College holds is accurate and kept up to date.

7.2 It is the responsibility of the Personnel to ensure their details with the College are up to date and accurate and to inform the College if there are any changes.

7.3 All College Personnel that collect and record Personal data shall ensure that the Personal data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

7.4 All College Personnel who obtain Personal data from sources outside the College shall take reasonable steps to ensure that the Personal data is recorded accurately, is up to date and limited to that which is adequate, relevant and necessary in relation to the purpose for which it is collected and used. This does not require College Personnel to independently check the Personal data obtained.

In order to maintain the quality of Personal data, all College Personnel that access Personal data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

7.5 The College recognises the importance of ensuring that Personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College will respond to queries and requests according to individual rights within one month and all queries should be directed to the data protection officer dpo@burycollege.ac.uk

8. Personal Data must not be kept longer than needed

8.1 Data Protection Laws require that the College does not keep Personal data longer than is necessary for the purpose or purposes for which the College collected it.

8.2 The College has assessed the types of Personal data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal data processed by the College, the reasons for those retention periods and how the College securely deletes Personal data at the end of those periods. These are set out in the Data Retention and Disposal Policy. This policy is updated annually.

8.3 If College Personnel feel that a particular item of Personal data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal data retention practices, they should contact the Data Protection Officer for guidance.

9. Data security

The College takes information security very seriously and the College has 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.

The College has an IT Security Policy which is being developed to sit alongside this data protection policy.

10. Data Breach

10.1 While 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 Procedure.

10.2 A Personal Data Breach (PDB) 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.

10.3 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, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom

ware, deleting Personal data in error, loss of access to Personal data stored on systems, inability to restore access to Personal data from back up, or loss of an encryption key; and

Integrity breach - where there is an unauthorised or accidental alteration of Personal data.

The College has a data breach procedure which can be accessed on the College's intranet in the data protection pages. This procedure outlines how the College will deal with a data breach and the timescales it will endeavour to meet. If you suspect a data breach, please consult this procedure and follow the steps outlined or email the data protection officer at dpo@burycollege.ac.uk

11. Appointing contractors who access the college's personal data

11.1 If the College appoints a contractor who is a Processor of the College's Personal data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

11.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

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

11.4 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 a representative of Bury College acting as the Controller, remain responsible for what happens to the Personal data.

11.5 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 the UK GDPR, EU GDPR, member state/nation with data protection adequacy data protection law.

11.6 In addition, the contract should set out:

11.6.1 The subject-matter and duration of the processing;

11.6.2 the nature and purpose of the processing;

11.6.3 the type of Personal data and categories of individuals; and

11.6.4 the obligations and rights of the Controller.

12. Individual Rights

12.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. The different types of rights of individuals which the College is required to honour are reflected in the following paragraphs.

12.2 Subject Access Requests

Individuals have the right under UK GDPR to ask a College to confirm what Personal data they hold in relation to them and provide them with the data. The College is required to provide this information within one Calender month (with a possible extension if it is a complex request). The College will not be able to charge a fee to comply with this request unless the request is considered Manifestly unfounded or excessive.

12.3 Right of Erasure (Right to be Forgotten)

12.3.1 This is a limited right for individuals to request the erasure of Personal data concerning them where:

12.3.1.1 the use of the Personal data is no longer necessary;

12.3.1.2 their consent is withdrawn and there is no other legal ground for the processing;

12.3.1.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;

12.3.1.4 the Personal data has been unlawfully processed; and

12.3.1.5 the Personal data has to be erased for compliance with a legal obligation.

12.3.2 In a marketing context, where Personal data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal data must not be processed for such purposes.

12.4 Right of Data Portability

12.4.1 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:

12.4.1.1 the processing is based on consent or on a contract; and

12.4.1.2 the processing is carried out by automated means

12.4.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

12.5 The Right of Rectification and Restriction

12.5.1 Finally, 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.

The College will use all Personal data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights under these laws.

13. Marketing and Consent

13.1 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 require that this is only done in a legally compliant manner.

13.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR And PECR has introduced a number of important changes for organisations that market to individuals, including:

13.2.1 providing more detail in their privacy notices, including for example whether profiling takes place; and

13.2.2 rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO prefers consent to be used in a marketing context. However, this is not a requirement if another lawful basis, or the “soft opt in” were to apply.

13.3 The College has a Privacy and Electronic Communications Regulations (PECR) Policy which will sit alongside this data protection policy. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data

13.4 The College will either use an un-ticked opt-in box for consent, or alternatively, the College may use a “soft opt in” if the following conditions are met:

13.4.1 contact details have been obtained in the course of a sale (or negotiations for a sale);

13.4.2 the College is marketing its own similar services; and

13.4.3 the College has given the individual a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

14. Automated decision making and profiling

14.1 Under Data Protection Laws there are controls regarding profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

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

14.2 Any Automated Decision Making or Profiling which the College carries is only be done once the College is confident that it is complying with Data Protection Laws. If College Personnel

therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

14.3 College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

14.4 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

15. Data Protection Impact Assessments (DPIA)

15.1 UK GDPR continues the requirement for data controllers to carry out a risk assessment in relation to the use of Personal data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal data but is an assessment of issues affecting Personal data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

15.2 A DPIA will be completed where the use of Personal data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk. In addition, the DPIA toolkit can be provided on request to the DPO. The College's DPIA can be found on the data protection pages of the intranet. The Data Protection Officer will be the final authorisation that a DPIA has been adhered to and assurance can be given. All DPIAs will be held central by the Data Protection Officer.

15.3 Where a DPIA reveals a high level of risk which cannot be appropriately mitigated the ICO must be consulted.

15.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

15.5 Where a DPIA identifies that a web-based College service is likely to be used by children we will also aim to ensure this complies with the Children's Code

15.6 Situations where the College may have to carry out a Data Protection Impact Assessment includes, but is not limited to:

15.6.1 large scale and systematic use of Personal data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

15.6.2 large scale use of Special Categories of Personal data, or Personal data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

15.6.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.

15.6.4 Introduction of an IT system which processes large amounts of personal data

16. The Age Appropriate Design Code

16.1 The College accepts and recognises that some of its web-based services are likely to be accessed by people under the age of 18. When this is the case particular emphasis and care must be taken to ensure compliance with the Age Appropriate Design Code (Children's Code).

16.2 Situations where this may apply include but are not limited to.

16.2.1 The provision of online based support services, such as web portals and college emails

16.2.2 Processing data in relation to submitting applications to enrol with the college

16.2.3 The use of any apps developed or used officially by Bury College that are likely to be used by under 18s

16.2.4 The College will monitor the development and usage of its web-based platforms and add further examples where appropriate.

16.3 When the College identifies that a service is likely to be used by children, either by a DPIA or other means, we will ensure that this services is operated in the best interests of the child, this will be done by.

16.3.1 Keeping them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;

16.3.2 Protect and support their health and wellbeing;

16.3.3 Protect and support their physical, psychological and emotional development;

16.3.4 Protect and support their need to develop their own views and identity;

16.3.6 Protect and support their right to freedom of association and play;

16.3.7 Support the needs of children with disabilities in line with our obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland;

16.3.8 Recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and

16.3.9 Recognise the evolving capacity of the child to form their own view, and give due weight to that view.

16.3.10 The College shall also ensure when providing a web-based service likely to be used by children that it follows the other principles of the age appropriate design code should they be relevant to the service. These can be found on the ICOs website

Commented [PM1]: by

Commented [PM2]: service is operated

17. International Transfers of personal data

17.1 Data Protection Laws impose strict controls on Personal data being transferred outside the UK . Transfer includes sending Personal data outside the EEA but also includes storage of Personal data or access to it outside the UK. It needs to be thought about whenever the College appoints a supplier outside the UK or the College appoints a supplier with group companies outside the UK which may give access to the Personal data to staff outside the UK.

17.2 So that the College can ensure it is compliant with Data Protection Laws College Personnel must not export Personal data unless it has been approved by the Data Protection Officer.

17.3 College Personnel must not export any Personal data outside the UK without the approval of the Data Protection Officer.

17.4 The College transfers personal information outside of the UK in the following circumstances

- with the British Council and/or country of origin for international students
- Eventbrite - administer your booking and facilitate your attendance at our event.
- Grofar – Administer and storage of data related to managing apprenticeships and placements

The college uses SCC (Standard contractual clauses) to check compliance with our Data Protection obligations, these replace Privacy Shield. For more information, please see our Privacy policy.

Equality Impact Assessment

Screening for effects on equality	
Name of policy being assessed.	Data Protection Policy
Policy Holder and/or person with authority to make changes to policy:	Oliver Mackenzie
Position:	DPO
Directorate:	Finance and Corporate Services
New/Revised/Reviewed Policy:	**Revised Policy**
What is the aim, objective or purpose of the policy, procedure, strategy or decision?	
To explain the responsibilities of students and staff with regard to data protection. Staff are data subjects and data processors Students are Data Subjects Bury College is the Data Controller.	
Who was consulted when the policy was first written?	
GDPR Consultant	
Who does the policy affect?	
Staff, Students, Governors and Clients (all data subjects)	
Who implements the policy, and what steps will be taken to ensure the effective implementation of the policy?	
Leadership Team, Managers, HR, Staff and DPO	
What pre-existing evidence is available to facilitate the screening of the policy?	
• Data Protection SAR log • Student Information Data request log • Data Protection Breach form • Data Protection Breach log	

What impact is the policy likely to have on the following characteristics?					
Protected characteristic*	**Positive impact**	**Negative impact**	**Neutral impact**	**Unclear**	**Further comments**
Age (or age group)	□	□	**x**	□	
Disability	□	□	**x**	□	
Gender reassignment	□	□	**X**	□	
Pregnancy and maternity	□	□	**X**	□	
Race (including ethnicity and nationality)		□	**X**	□	
Religion or belief	□	□	**X**	□	
Sex	□	□	**X**	□	
Sexual orientation	□	□	**X**	□	
Marriage/Civil Partnerships	□	□	**X**	□	
Looked after learners	□	□	**X**	□	
Social-economic	□	□	**X**	□	
Carers	□	□	**X**	□	
Ex-offenders	□	□	**X**	□	

***Protected Characteristics as identified by the Equality Act 2010.**

If any answers are 'negative' can any adverse impact be justified on the basis of a legal requirement? Yes ☐ No ☐

If 'yes', please explain:

Please detail any suggested actions identified to improve positive impact or remove negative impact of this policy.

Issue identified	Suggestion action to address this issue

Should a Full Equality Impact Assessment be carried out? No

How will this policy be approved? Leadership Team and Resources Committee

Name & Signature	Oliver Mackenzie O.J.Mac
Date	24th October 2022