Burton and South Derbyshire College

Creating the skills of tomorrow.

Data Protection Policy

www.bsdc.ac.uk

Policy Title	
Policy Summary	This Policy sets out the basis on which the College will collect and use personal data either where the College collects it from individuals, or where it is provided to the College by authorised third parties. It also sets out rules on how the College handles, uses, transfers, and stores personal data.
Policy Owner	Deputy Principal Curriculum Quality & IT Services
Policy Version	V1.0
Approved By	Senior Leadership Team (SLT)
Date Approved	June 2024
Distribution	External
Review Date	September 2027
Equality Impact Assessment	Completed June 2024 (available on request)
Noted Changes / Amendments	
Approval Date: June 2024	New Policy Changes to roles and responsibilities
Linked Policy/Documents	
BSDC Record Retention Policy – Internal Document BSDC Data Breach Response Plan & Protocol – Internal Document	

Contents

1. POLICY DEFINITION 3
2. OVERVIEW 4
3. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS 4
4. DATA PROTECTION PRINCIPLES 4
5. LAWFUL USE OF PERSONAL DATA 5
6. TRANSPARENT PROCESSING – PRIVACY NOTICES 5
7. DATA QUALITY 5
8. PERSONAL DATA RETENTION 6
9. DATA SECURITY 6
10. DATA BREACH 7
11. APPOINTING CONTRACTORS (DATA PROCESSORS) 8
12. INDIVIDUALS' DATA RIGHTS 9
13. MARKETING AND CONSENT 9
14. AUTOMATED DECISION MAKING AND PROFILING 9
15. DATA PROTECTION IMPACT ASSESSMENTS (DPIA) 10
16. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA 10

Equality Impact Assessment (EIA) (Internal Publication ONLY) ..... **Error! Bookmark not defined.**

1. POLICY DEFINITION

The College	Burton & South Derbyshire College (BSDC)
Data Protection Officer	Burton & South Derbyshire College (BSDC) Data Protection Officer: Deputy Principal Curriculum, Quality & IT Services: DP.Officer@bsdc.ac.uk 01283 494400
College Personnel	Any college employee, who accesses any of the College's Personal Data and will include consultants, contractors, and temporary personnel hired to work on behalf of the College.
Data 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.
Data Protection Laws	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'
Data Protection Officer	Burton & South Derbyshire College (BSDC) Data Protection Officer: Deputy Principal Curriculum, Quality & IT Services: DP.Officer@bsdc.ac.uk 01283 494400
EEA	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the UK.
ICO	Information Commissioner's Office, the UK's data protection regulator. https://ico.org.uk
Individuals	Living individuals who can be identified, *directly or indirectly*, from information that the College has.
Personal Data	Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
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.
Special Categories of Personal Data	Personal Data that reveals a person's race 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 and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) is a process to help entities identify and minimise the data protection risks.

2. OVERVIEW

As an organisation that collects, uses, and stores personal data about its learners, apprentices, employees, suppliers, parents and visitors, the College recognises that having controls around the collection, use, retention, and destruction of personal data is important in order to comply with its obligations under Data Protection Laws and in particular its obligations under Article 5 of the General Data Protection Regulations (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.

All members of College Personnel are obliged to comply with this policy at all times.

Any queries relating to this policy or use, retention and destruction of personal data should contact the College's Data Protection Officer (DPO), who is responsible for ensuring the College's compliance.

3. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

(3.1) All College personnel must comply with this policy. College personnel must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.

(3.2) College personnel must not release or disclose any personal data outside the College, or College personnel without specific authorisation from their line manager or the DPO.

(3.3) College personnel must take all steps to ensure there is no unauthorised access to personal data whether by unauthorised College Personnel or by people outside the College.

4. DATA PROTECTION PRINCIPLES

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

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary for the purposes for which it is being processed.
- 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.
- Kept for no longer than is necessary for the purposes for which it is being processed; and 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.

5. LAWFUL USE OF PERSONAL DATA

(5.1) 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.
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

(5.2) 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.
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

(5.3) 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.

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.

(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 and in any event within one month.

(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

(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) 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.

(7.3) All College personnel that 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 limited to what is 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.

(7.4) 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 has a rights of Individuals policy and a rights of Individuals procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure, or restriction of the use of their personal data should be dealt with in accordance with those documents.

8. PERSONAL DATA RETENTION

(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 Record Retention Policy.

(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 Record 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

(9.1) The College takes information security very seriously and has security measures to prevent unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

(9.2) 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.

(9.3) All college personal are responsible for ensuring that any personal data which they hold or have access to is held securely and not disclosed either verbally, in writing, accidentally or otherwise to any unauthorised third party. The following general guidance should be followed:

- Paper-based data should be kept in a locked cabinet or drawer within a locked room.
- Computerised data and records should be stored in designated secure digital location only. This includes BSDCs physical onsite digital storage areas and Microsoft Office 365 cloud data storage (SharePoint).
- All BSDC mobile devices (laptops, tablets, and smart phones) should be suitably encrypted, or protected against by authorised access.
- When sending personal data outside of the College to 'data processor', this data must be password protected. The password must then be transported via separate means directly to the recipient.
- Data should never be stored at a staff member's personal residents or outside of a recognised BSDC designated work location, whether in paper or electronic forms, unless on an encrypted device or within approved cloud storage locations (e.g., BSDC's Microsoft SharePoint).
- Data (paper based or digital) should be held in accordance with BSDC Record Retention Policy.

10. DEALING WITH DATA BREACH

(10.1) The College will act diligently at all times and takes its responsibility of controlling data seriously but acknowledges that in today's world it would be impossible to provide absolute assurances, recognising data security breaches could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data.

(10.2) 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.

(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, 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 learner or apprentice, 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 ransomware, 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.

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

(10.4) Where there is a suspected or known data breach, by law, the College is obligated to report this to the ICO and relevant authorities (where required) without undue delay and within 72 hours (if the incident meets the threshold for reporting). During this period the College will make best efforts to recover any data or contain any further breaches of personal data following its data breach response plan and protocol.

11. APPOINTING CONTRACTORS (DATA PROCESSORS)

(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) The requirement of GDPR is that the 'Data 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. Any contract where an organisation appoints a 'Processor' must be in writing.

(11.3) You are considered as having appointed a 'Processor' where you engage someone to perform a service for you and as part of this, they may get access to your personal data. Where the College appoints a 'Processor' the College, as 'Data Controller' remains responsible for what happens to the personal data.

(11.4) GDPR legislation 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 GDPR or other data protection law.

(11.5) 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'.

12. INDIVIDUALS' DATA RIGHTS

Individuals' data rights can be found in our Rights of Individuals Policy.

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 will bring about a number of important changes for organisations that market to individuals, including:

- providing more detail in their privacy notices, including for example whether profiling takes place; and
- rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

(13.4) The College also needs to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. 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.

(13.5) Consent is central to electronic marketing, and this will only be obtained by providing an un-ticked opt-in box. Alternatively, the College may be able to market using a "soft opt in" if the following conditions were met:

- contact details have been obtained in the course of a sale (or negotiations for a sale).
- the College are marketing its own similar services.
- the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

14. AUTOMATED DECISION MAKING AND PROFILING

Under data protection laws there are controls around profiling and automated decision making in relation to Individuals.

(14.1) **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.

(14.2) **Profiling** happens where the College automatically uses personal data to evaluate certain things about an individual.

- Any automated decision making or profiling which the College carries out can 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.

- College personnel must not carry out automated decision making or profiling without the approval of the Data Protection Officer.

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

15. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

(15.1) The GDPR introduce a new requirement 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).

(15.2) 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 measures to address the risks.
- A DPIA must be completed where the use of personal data is likely to result in a high risk to the rights and freedoms of individuals.
- Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.
- 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.
- Situations where the College may have to carry out a DPIA include the following:
    - 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.
    - 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
    - Systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- All DPIAs must be reviewed and approved by the Data Protection Officer.

16. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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

(16.2) 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.

(16.3) College personnel must not export any personal data outside the EEA without the approval of the Data Protection Officer.