Policy Name	Data Protection Policy
Department	College Information Services
Created By (Job Title)	Director of College Information Services
Date Reviewed	April 2022
Date of Next Review	March 2024
Pathway	
E & D Policy Disclaimer	This policy has been reviewed in line with the Equality Act 2010 which recognises the following categories as Protected Characteristics: Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender) and Sexual orientation. We will continue to monitor this policy to ensure that it provides equal access and does not discriminate against anyone, especially any person/s listed under any protected characteristic. ***17.03.20***

Data Protection Policy

1. About this policy

The Bedford College Group ("TBCG") (here-after referred to as the College) is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

The General Data Protection Regulations (GDPR) demands higher transparency and accountability in how we as a College manage personal data. It also gives new and stronger rights for individuals to understand and control the use of their personal data.

As an organisation that collects, uses and stores personal data about its prospective applicants, students and their parents/guardians, employees, governors and commercial customers, we recognise that having effective controls around all aspects of personal data is essential in order to demonstrate compliance with data protection legislation.

Protecting the confidentiality and integrity of Data is a key responsibility of all College Personnel and those working on its operations.

2. Policy Statement of TBCG

TBCG's policy is to comply with the Data Protection Act 2018 ("DPA"), The General Data Protection Regulation (EU) 2016/679) ("GDPR") and any national implementing laws and regulations relating to the processing of Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other national data protection authority.

As a group we need to collect and use certain types of information about people with whom we deal in order to operate. These include current, past and prospective employees, volunteers, learners, prospective learners, parents, alumni, suppliers, clients/customers, and others with whom it communicates.

In addition, we are required by law to collect and use certain types of information of this kind to comply with the requirements of government departments.

This Personal Data and Special Category Personal Data (together referred to for the purposes of this Policy as "Data" (See Section 9 and 10) must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on any other material.

We recognise and regard the lawful and correct treatment of Data as extremely important within our day to day functions and in treating those with whom we deal with respect and professionalism ensuring their confidence in our ability at all times.

All staff, volunteers, Governors of TBCG and other parties under contract are required to handle data accessed / obtained in accordance with this Policy.

3. Scope

This Policy applies:

- To the Bedford College Group ("TBCG"), meaning all businesses which form part of TBCG, including but not limited to Bedford College, National College for Motorsport, Shuttleworth College, the Bedford Sixth Form, Tresham College and wholly owned subsidiaries of Bedford College, Bedford College Services Limited and Bedford College Professional Services Limited.

- To all staff (including temporary and agency workers, contractors and volunteers) and Governors across the Group.

- To all data held on behalf of the College, regardless of where the data is held i.e. if the personal data is held on personally-owned equipment or outside College property.

- To any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV), and sound recordings.

4. TBCG Personnel responsibilities

All TBCG Personnel are obliged to comply with this Policy, the Data Management procedures and other relevant policies at all times.

For the avoidance of doubt and for the purpose of this Policy "TBCG Personnel" includes any employee, worker or contractor who accesses any of TBCG's Data and will include employees, consultants, contractors and temporary personnel hired to work on behalf of TBCG.

TBCG Personnel must ensure that they keep confidential all Data that they collect, store, use and come into contact with during the performance of their duties.

TBCG Personnel must not release or disclose any Data, either internally or externally, to any unauthorised parties without specific authorisation from their manager or the DPO; this includes by phone calls or in emails.

TBCG Personnel must take all steps to ensure there is no unauthorised access to Data by any unauthorised personnel (internal or external).

5. Data Protection Officer

We have appointed a Data Protection Officer for TBCG who will endeavour to ensure that all Data is processed in compliance with this Policy and the Principles of the Data Protection Act 2018 ("DPA"). The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

6. Third-Party Data Processors

Where external companies are used to process personal data on behalf of the College, responsibility for the security and appropriate use of that data remains with the College.

Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken to determine that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;
- a data processing agreement, must be signed by both parties.

7. Contractors, Short-term, Voluntary Staff and Governors

The College is responsible for the use of personal data by anyone working on its behalf.

Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing.

In addition, managers will ensure that:

- any personal data collected or processed in the course of work undertaken for the College is kept securely and confidentially;
- any access to data is revoked once they no longer need access
- all personal data is returned to the College on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and the College receives notification in this regard from the contractor or short term / voluntary member of staff;
- the College receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- any personal data made available by the College, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the College;

- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

The above points are also applicable to Governors.

8. The Principles

We will fully endorse and adhere to the principles within the Data Protection Act 2018 and ensure that personal data shall be:

1. Processed fairly and lawfully and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with that purpose.
3. Adequate, relevant and limited to what is necessary for that purpose.
4. Accurate and, where necessary kept up to date
5. Kept in a form that permits identification for no longer than necessary
6. Processed in a manner that ensure appropriate security.

The College has a number of policies and procedures in place, including this Policy to ensure that the College and its staff adhere to these principles and can demonstrate compliance.

9. Personal Data

Personal Data covers both facts and opinions about an individual where that data identifies or in conjunction with other information an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary or a pupil's attendance record and exam results. Personal data may also include sensitive personal data as defined in the Act.

10. Special Category Personal Data

Special Category Personal Data includes data relating to medical information, gender, religion, philosophical beliefs, race or ethnic origin, sexual life or sexual orientation, trade union membership, political opinions, genetic data (i.e. information about physical, physiological or behavioural Characteristics such as facial images and fingerprints), physical or mental health and criminal records and proceedings

For the purposes of this Policy Personal Data and Special Category Personal Data will together be referred to as **"Data"**

11. Processing of Data

Through appropriate management the Group will:

- fully observe our legal obligations regarding the fair collection and use of information;
- obtain appropriate consent for the processing of Data unless processing does not require consent
- meet our legal obligations to specify the purposes for which information is used and apply suitable privacy notices;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- ensure that where Data is processed by external processors, for example, service providers, cloud services including storage, web sites etc. the appropriate data protection clauses/agreements are in place.
- retain Data for different periods of time in accordance with legal requirements or best practice and apply checks to determine the length of time information is held and ensure compliance with the College's Data Retention Policy.
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken: the right of access to one's Data; the right to prevent processing in certain circumstances; the right to rectify, block or erase information which is regarded as wrong information.);
- take appropriate technical and organisational security measures to safeguard Data;
- ensure that are appropriate process to consider the impact of processing activities to data Subjects.
- ensure that Data is not transferred abroad without suitable safeguards.
- ensure when Data is destroyed, it is destroyed only where appropriate and securely in accordance with best practice at the time of destruction

In addition, we will ensure that:

- there is someone with specific responsibility for data protection in the organisation;
- everyone managing and handling Data understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling Data is appropriately trained to do so;
- there are details of how to make enquires which are available on our external website and staff intranet pages.
- queries about handling Data are promptly and courteously dealt with;
- a regular review and audit is made of the way Data is managed;
- methods of handling Data are regularly assessed and evaluated.

12. Enforcement and breach management

If an individual believes that we have not complied with this Policy or acted otherwise than in accordance with Data Protection Principles, the individual should notify the DPO immediately at dataprotection@bedford.ac.uk.

We have a legal obligation to notify the Information Commissioner of any breach or suspected breach of Data Protection legislation (considered to be high risk) within 72 hours of the breach or suspected breach.

If you know, suspect or are unsure if a personal data breach has occurred, you should immediately contact the Data Protection Office via dataprotection@bedford.ac.uk or complete the incident reporting form on the intranet. You will then be advised the next steps to take.

13. Other relevant policies and procedures

The following Policies and procedures and others shall be adhered to by all those processing Data at TBCG;

- Data Management Policy (including Breach notification form and Subject Access Request form,
- ICT Systems Acceptable Use Policy
- Relevant Employee related policies
- Relevant Student related policies
- Network Security Policy
- Mobile Devices and Laptops Policy
- Privacy Policy
- Data Retention Policy / guidelines
- Freedom of Information Policy
- Raising Concerns Procedure
- Special Category Personal Data Policy

For further information and guidance concerning TBCG's responsibilities in respect of data protection please email mydata@bedford.ac.uk