“Inspiring learning, developing character, building futures”

MIEX policies and procedures

Data Protection Policy

(Including GDPR Compliance)

Aim: The Blackpool Sixth Form College is required to keep and process personal information about staff, students, contractors, visitors, governors and others. We recognise that having controls around the collection, use, retention and destruction of personal data is important in order to comply with our obligations under data protection laws and in particular our obligations under Article 5 of the General Data Protection Regulation (GDPR).

Policy authorisation:	Management: Senior Leadership Team
Date of policy introduction or most recent update:	August 2023
Date of next policy review:	August 2025
Policy author:	Data Protection Officer (Head of MIEX)

1. Introduction

1.1. The Blackpool Sixth Form College is required to collect, store and process personal data in order to carry out its functions and activities as a college and all staff members within the college are committed to protecting the confidentiality and integrity of the personal information it collects in line with the new GDPR legislation. The college recognises the importance of data protection and is committed to protecting and safeguarding personal data. The college collects, stores and processes personal data on a variety of stakeholders in order to carry out its activities and functions.

1.2. As an organisation that collects, uses and stores personal data about its employees, students, suppliers, partners, directors, parents and visitors, the college recognises that having controls around the collection, use, retention and destruction of personal data is important to comply with the college's obligations under data protection laws and in particular its obligations under Article 5 of GDPR.

1.3. 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. College personnel will be signposted to this policy when they start and will receive periodic revisions of this policy as deemed required as part of the review process. 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.
A glossary of terms is available in Appendix 2.

1.4. The college's Data Protection Officer is responsible for informing and advising the college and it's staff on its data protection obligations and for monitoring compliance with these obligations and this policy. If you have any questions concerning the content of this policy or if you need further information, please contact our Data Protection Officer, by post

Data Protection Officer
The Blackpool Sixth Form College
Blackpool Old Road
Blackpool
FY3 7LR

or via email: dpo@blackpoolsixth.ac.uk

2. Scope of the policy

2.1. This policy sets out the basis on which the college will collect and use personal data either where the college collects it from individuals itself, 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. The policy is in place to ensure that college personnel are aware of their responsibilities under data protection laws. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within The Blackpool Sixth Form College and as such we are obliged to comply with this policy at all times to minimise the potential risk of damage and distress to individuals (data subjects) and also the risk of penalties, fines, legal action and reputational damage to our organisation.

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

2.3. This policy will be updated as necessary to reflect best practice, or amendments made to the data protection legislation, and shall be formally reviewed and approved every two years

3. Definitions

3.1. **Personal Data** – any information that can be related to an identified or identifiable living person (referred to as a data subject).

3.2. **Special Categories of Personal Data –** personal data that reveals a person's

- racial or ethnic origin;
- political opinions:
- religious or philosophical beliefs;
- trade union membership;
- genetic data, biometric data;
- physical or mental health;
- sexual life or sexual orientation.

3.3. These special categories of personal data are subject to additional controls in comparison to ordinary personal data. Staff or students are under no obligation to disclose data under these categories (save to the extent that marital details and / or parenthood are needed for other purposes e.g. pension entitlements.)

3.4. Information relating to criminal convictions shall only be held and processed where there is a legal authority to do so.

3.5. **Controller** – any entity (e.g. company, organisation or person) that determines the purposes for which, and the manner in which, any personal data is processed.

3.6. **Processor** – any entity (e.g. company, organisation or person) that processes personal data on behalf of a controller (e.g. the college).

4. General responsibilities of college personnel

All those within The Blackpool Sixth Form College must comply with this policy and:

4.1. 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.

4.2. **must not** release or disclose any personal data to anyone not authorised to access the personal data internally or outside The Blackpool Sixth Form College (**this includes phone calls and emails**).

4.3. must take all steps to ensure there is no unauthorised access to personal data whether by others within The Blackpool Sixth Form College who are not authorised to see such personal data or by people outside the organisation.

5. Training

5.1. All new starters are required to complete an online externally produced training module '**A Guide to UK Data Protection: Education**'

5.2. Internal training/notices ares released periodically i.e. Cyber Security, password security, multi factor authentication, phishing etc

6. Accountability

The GDPR requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".
This is the concept of 'accountability'. Accountability requires compliance with the principles in Section 3 of this policy (and Article 5 of the Data Protection Act 2018). It is not enough to comply; the college has to be able to demonstrate compliance through documentation such as this policy, privacy notices and procedures.

7. Data protection principles

7.1. When using personal data, data protection laws require that the college complies with the following **six principles** and that personal data must be:

7.1.1 Processed lawfully, fairly and in a transparent manner and processing shall not be lawful unless one of the processing conditions can be met.	The college must be transparent with individuals (data subjects) about how the college will use their personal data. This is generally done through our privacy notices. The information that needs to be provided is set out in Article 13 and 14 of GDPR
7.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	Personal data must not be collected for one reason and then processed for another unless we have informed the individual. Our privacy notices will normally specify that some personal data may be used for a variety of purposes.
7.1.3 Adequate, relevant and limited to what is necessary for the purposes for which it is being processed.	Personal data collected must be necessary for the purposes for which it is being processed and not be collected “just in case” and forms that are used to collect data will be reviewed periodically to determine whether any sections can be made optional.
7.1.4 Accurate and kept up to date, meaning every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible.	The college recognises that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible and understanding the purpose for which personal data has been collected and is being used and ensuring that irrelevant personal data is not collected. This is known as data minimisation. Checks will be carried out on a regular basis to ensure that the data held is accurate. If the data is inaccurate or has changed, the college will take steps to make sure that it is erased or rectified. It is however the responsibility of the individual to ensure the college and 3rd party data storage is kept updated with changes to personal data.
7.1.5 Kept for no longer than is necessary for the purposes for which it is being processed.	The college should not keep personal data for longer than it is needed. This is not a “one size fits all” basis and when personal data is no longer needed, it should be securely deleted/destroyed in accordance with retention periods outlined in the Retention Schedule Annex to this policy. Some records relating to former students or employees may

	be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
7.1.6 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.	It is a requirement of GDPR that appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage of personal data. We take security very seriously and have in place policies, procedures and technologies to maintain the security of personal data. In recent years focus on improving cyber security, multi factor authentication, password convention and protection

7.2. The college is committed to complying with the principles in 7.1 at all times which means the college will:

7.2.1 Inform individuals as to the purpose of collecting any information from them, through the use of Privacy Notices which are issued at application.	● The ESFA provides a Privacy Notice which students must be shown and this is done through the applications platform and the Enrolment Gateway. ● The College also has Privacy notices for its stakeholders, including students, parents, vacancy applicants, staff etc.
7.2.2 Be responsible for checking the quality and accuracy of information.	● Student data is rigorously checked from the point of enrolment to qualification completion, ● Employee data is rigorously checked through application, appointment and the term of employment.
7.2.3 Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with data retention guidance.	● Data retention and disposal schedule in place
7.2.4 Ensure that when information is authorised for disposal it is done appropriately.	● Confidential Waste Procedures for staff ● Retention and disposal schedule ● Shredding facilities available around college ● Confidential waste contract in place for disposal of hard copy documentation

7.2.5 Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on the college's computer system, and follow the relevant security policy requirements at all times.	• Multi Factor authentication adopted where possible • password policy • Locking filing cabinets for hard copy documents • Firewall in place • Data protection training • Data Protection Officer in college • Cyber security credentials
7.2.6 Share personal information with others only when it is necessary and legally appropriate to do so.	• Data Protection disclosure procedures in place • Safeguarding Policy in place • Data Protection training and policy
7.2.7 Set out clear procedures for responding to requests for access to personal information known as subject access requests.	• Data Protection policy and procedures in place • Data Protection Officer responds to SARs
7.2.8 Report any breaches of the UK GDPR in accordance with the procedures in section 18 below.	• Data breaches are reported to the DPO • Clear Data Breach procedure in place Annex 3 of Data Protection policy

8. Personal data and special categories of data

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria:

'Personal Data' is clearly defined in Article 6 of GDPR	Any information relating to a 'living/identifiable person' (data subject) who can be directly or indirectly identified by reference to an identifier e.g name, roll number, location data or online identifier, any information which relates directly to an individual and can be linked directly to them.
Special categories of 'personal data' are clearly defined in Article 9 of the GDPR	The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal offence and convictions data	This does not fall in the scope of personal data but there are restrictions in processing defined in Article 10
Pseudonymised personal data	Data which has been pseudonymised can only be connected back to an individual using a specific key or code. This can be an extra layer of security, but the data is still treated as personal data under GDPR because of the possibility of personal identification.
Anonymised personal data	Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by organisations to conduct research. Full anonymised data is not covered by GDPR as it contains no personal identification.

For the purpose of this policy, personal data refers to information that the college collects and processes; for example, it relates to an identifiable, living individual for example a member of staff who could be identified directly or indirectly by gender, job role and office location if you can work out who they are. In our organisation, the college will process personal data and in some cases special categories of data and criminal conviction and offence data for the following individuals (data subjects), these are explained in more detail within our privacy notices:

- Employees (current and former)
- Employee next of kin/emergency contact
- Recruitment candidate
- Directors
- Volunteers
- Work experience student or intern
- Students (current and former)
- Parents/Guardians/Carers/Emergency Contacts
- Contractors/Subcontractors
- Consultants/Freelancers
- Training delegates
- Customers/clients/service users
- Visitors
- Members of the public

9. Lawful processing of personal data

9.1. The college lawfully processes personal data under the legal basis set out in Article 6 of the GDPR. In order to collect and/or use personal data lawfully, and in accordance with the first principle defined in 7.1 above, the college needs to be able to demonstrate that its use meets one of a number of legal grounds.

Lawful basis	Examples
9.1.1 **Contractual obligation**	The processing is necessary for a contract we have with an individual or third party or specific steps we are asked to take before entering into a contract *e.g. terms and conditions of employment/payroll info and supplying goods and services to organisations*
9.1.2 **Legal obligation**	The processing is necessary for us to comply with the law (not including contractual obligations). There are many lawful obligations which we must fulfil e.g. tax/pension/compliance with Health & Safety at Work Act/Equality & Diversity/providing education to under 18s etc. We must process personal data lawfully if the data processing falls within this category, however, in most cases Public (Task) Interest will also apply.
9.1.3 **Vital interest**	The processing is necessary to protect someone's life. Emergency information *e.g. in cases of life or death.*
9.1.4 **Public interest (task)**	The processing is necessary for the performance of a task carried out in the public interest and is necessary for the administration of justice or rule of law.
9.1.5 **Legitimate interest**	The processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's (data subject's) personal data which overrides those legitimate interests. As a public body, we cannot rely on the lawful purpose of legitimate interests where the processing is in the performance of a task carried out in the public interest or in the exercise of official authority e.g. our core activities. Instead, we need to rely on the processing being necessary for the performance of a task carried out in the public interest. We may use it for areas such as marketing, fundraising or selling items such as tickets for events and equipment.
9.1.6 **Consent**	The individual (data subject) has given clear consent for us to process their personal data for one or more specific purposes *e.g. photographs/videoing, academic results and achievement, biometric data, and using details for marketing activities.*
	Consent must be: ● freely given ● specific ● informed ● an unambiguous indication of an individual's (data subjects) wishes ● a form of firm confirmation or positive opt-in, such as ticking boxes on a webpage ● easily able to be withdrawn

Consent, cannot be obtained from the following:

- silence
- pre-ticked boxes
- inactivity

Consent cannot be used in an employer and an employee relationship. The reasoning behind this is that the relationship is imbalanced and so the employee cannot really refuse to give their consent, for similar reasons, we may find consent difficult to rely on wherever there is a position of power e.g. over students.

Marketing and consent

The college may sometimes wish to contact individuals to send them marketing or promotional materials, the college will do this in a legally compliant manner by providing detail in their privacy notices, including for example whether profiling takes place and the college will ensure that we obtain an individual's "clear affirmative action" giving un-ticked opt-in boxes. The college will also consider other data privacy laws which sit alongside data protection in relation to direct and electronic marketing. The college will follow ICO Marketing Guidance.

The college will keep records documenting how and when consent was given, these may be held in a variety of storage mechanisms depending on the type of data and/or consent required. This information will be readily available for staff to check that consent has been obtained e.g. use of student photographs.

Children's consent

When offering an online service directly to a child, only children aged 13 or above are able to provide their own consent. For children under this age, you need to get consent from the person who has parental responsibility. Where a child is under the age of 13, where necessary consent will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child. Consent in terms of the use of a child's personal data is different to the consent required for participation in college events and activities for children where parental or legal guardian consent may be required to take part for insurance, safeguarding or health and safety reasons.

Withdrawal of consent

"Consent" can be withdrawn by the individual at any time. It is therefore extremely important that due consideration is given to any processing activities whereby data is shared or processed and becomes outside the control of The Blackpool Sixth Form College, for example printed materials, press releases etc. as the college will be unable to exercise certain individual rights. In these instances, specific "informed"

	consent will need to be obtained.

10. Lawful purposes for processing 'special categories of personal data'

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 are as follows (paraphrased):

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

11. Transparent Processing – Privacy Notices

11.1. Where the college collects personal data directly from individuals, the college will inform them about how the college uses their personal data in a privacy notice. These notices are available on the college websites and are subject to regular review.

12. Data Quality

12.1. 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. The college is also required to ensure that the personal data that it holds is accurate and kept up to date.

12.2. The college will take reasonable steps to ensure that personal data is recorded accurately, is kept 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.

12.3. The college will ensure that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection laws.

13. Data Retention

13.1. 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.

13.2. 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 and the reasons for those retention periods. (see Appendix 4 Data Retention Schedule)

14. Individuals (data subjects) rights under the GDPR

14.1. Individuals (data subjects) have certain rights under the GDPR; these rights are explained below together with details of how the college will ensure these rights are met:

14.1.1 **The right to be informed/sharing personal data (privacy notices)**	The GDPR requires us to inform individuals (data subjects) of our personal data processing activities, the college will do this through: ● Student Privacy Notice ● Employee, Director and Volunteer Privacy Notice ● Parent/Guardian/Carer and Third Party Privacy Notice ● Employer Privacy Notice	Privacy notices are available on the Blackpool Sixth Form College website. Paper versions are available on request.
14.1.2 **The right of access**	● Individuals (data subjects) have the right to obtain confirmation that their data is being processed and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes. Subject Access Requests should be made via the Data Protection Officer	
14.3 **The right to rectification**	Individuals (data subjects) are entitled to have inaccurate or incomplete	

	personal data rectified upon request via the Data Protection Officer. Upon receiving a request for rectification, the college will: ● check the validity of the request e.g. confirm the identity of the person requesting the change ● if the request is valid, amend the information where possible and record the actions taken ● where the personal data in question has been disclosed to third parties, the college will inform them of the rectification where possible and where appropriate, the college will inform the individual about the third parties that the data has been disclosed to ● the college will aim to deal with requests for rectification as soon as possible. The college will respond within one month; this will be extended by two months where the request for rectification is complex ● where the college makes a decision to take no action in response to a request for rectification, the college will explain the reason for this to the individual, and will inform them of their right to complain to the ICO	
14.1.4 **The right to erasure (the right to be forgotten)**	Individuals (data subjects) hold the right to request the erasure (deletion) or removal of personal data where there is no lawful basis for its continued processing, or request via the DPO in the following circumstances: ● Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed ● When the individual withdraws their consent ● When the individual objects to the processing and there is no overriding legitimate interest for	**The college will aim to deal with the right to erasure requests within one month,** where we are unable to complete the request within this timescale, the college will inform the individual.

	continuing the processing ● The personal data was unlawfully processed ● The personal data is required to be erased in order to comply with a legal obligation ● The personal data is processed in relation to the offer of information society services e.g. selling goods or services online to a child ● 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.	
	The college has the right to refuse a request for erasure where the personal data is being processed for the following reasons: ● to exercise the right of freedom of expression and information ● to comply with a legal obligation for the performance of a public interest task or exercise of official authority ● for public health purposes in the public interest ● for archiving purposes in the public interest, scientific research, historical research or statistical purposes ● the exercise or defence of legal claims. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. ● where personal data has been made public within an online environment, the college will inform other organisations who process the personal data to 'wherever' possible erase links	

	to and copies of the personal data in question. ● the college may not be able to exercise the right to erasure where content has been downloaded or re-shared. ● where personal data has been used for printed materials such as marketing leaflets and prospectuses, the college may no longer have control once published and therefore may not be able to exercise the right to erasure, where this is likely to apply the college will state this in our request for consent. ● where it is deemed that an adult or a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention must be given to existing situations where consent to processing has been given and they later request erasure of the data, regardless of age at the time of the request.	
14.1.5 **The right to restrict processing** Individuals (data subjects) have the right to request us to block or suppress processing of their personal data.	If a request is determined to be valid, the college will take steps to immediately restrict processing of personal data in the following circumstances: ● where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data ● where an individual has objected to the processing and we are considering whether our legitimate grounds override those of the individual ● where processing is unlawful and the individual opposes erasure and requests restriction instead ● where the college no longer need the personal data but the individual requires the data to establish, exercise or defend a	Where a restriction may affect The Blackpool Sixth Form College carrying out their legal and contractual obligations or it is believed that the data is being processed under the Public Interest, Vital Interest or Legitimate Interest conditions of processing, the college will follow guidance from the Information Commissioner's Officer to determine whether the request is valid and where possible temporarily stop processing until

	legal claim. ● if the personal data in question has been disclosed to third parties, the college will inform the third party about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.	the validity of the request is determined. Where processing is restricted, The Blackpool SIxth Form College will store the personal data, but not further process it guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The Blackpool Sixth Form College will inform individuals (data subjects) when a restriction on processing has been lifted as is practically possible.
14.1.6 **The right to data portability** Individuals (data subjects) have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. In the event that the personal data concerns more than one individual, the college will consider whether providing the information would prejudice the rights of any other individual.	The right to data portability only applies in the following cases: ● to personal data that an individual has provided to a controller ● where the processing is based on the individual's consent or for the performance of a contract ● when processing is carried out by automated means Personal data will be provided in a structured, commonly used and machine-readable form, free of charge, and where feasible, data will be transmitted directly to another organisation at the request of the individual. Requests should be made to the Data Protection Officer. Upon receipt the college will:	The college is not required to adopt or maintain processing systems, which are technically compatible with other organisations.

	● Respond with within one month or; ● Within one month advise the individual if the college needs to extend the timeframe by two months, where the request is complex, or a number of requests have been received ● Where no action is being taken in response to a request, the college will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO.	
14.1.7 **The right to object** The college will inform individuals (data subjects) of their right to object at the first point of communication, and this information will be outlined in our privacy notices and explicitly brought to the attention of the individual (data subject), ensuring that it is presented clearly and separately from any other information. Where possible the college will provide mechanisms for you to exercise your right to object, contact details within consent requests and privacy notices. The college will aim to deal with requests within one month and advise you if we cannot meet this timescale.	Individuals (data subjects) have the right to object to the following: ● Processing based on legitimate interests or the performance of a task in the public interest ● Direct marketing ● Processing for purposes of scientific or historical research and statistics. Where personal data is processed for the performance of a legal task or legitimate interests: ● an individual's grounds for objecting must relate to his or her particular situation. ● the college will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims or where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual. Where personal data is processed for direct marketing purposes: ● the college will stop processing personal data for direct	Where the processing activity is outlined as here, but is carried out online, the college will offer a method for individuals (data subjects) to object online.

	marketing purposes as soon as an objection is received. ● the college cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes. **Where personal data is processed for research purposes:** ● the individual must have grounds relating to their particular situation in order to exercise their right to object. ● where the processing of personal data is necessary for the performance of a public interest task, the college is not required to comply with an objection to the processing of the data.	
14.1.8 **Profiling and automated decision making** Profiling and automated decision making are two different things although automated decision making can include profiling. The college will specify any profiling or automated decision making in our privacy notices.	● **Profiling** happens where the college automatically uses personal data to evaluate certain things about an individual e.g. any element of analysing or predicting behaviours or preferences (e.g. staff utilisation reports, analysis of performance at work). Profiling can therefore happen even if the ultimate decision is not taken by a machine ● **Automated decision making** is where a decision is made about an Individual based solely on automated means without any human involvement and the decision has legal or other significant effects. Individuals (data subjects) have the right not to be subject to a decision when: ● it is based on automated processing, e.g. profiling ● it produces a legal effect or a similarly significant effect on the individual	Every student who enrols at college is required to undertake Lucid testing and the outcome scores are used to indicate potential Additional Learning Support options which are then discussed with the individual. Targeted cohorts of students (e.g. students who have had previously had exam arrangements in place at school) undertake Lucid Exact testing during the induction period. The outcome scores are used to indicate additional support needs which are then discussed with the individual.

	The college will take steps to ensure that individuals (data subjects) are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.	

15. Privacy by design and data protection impact assessments (DPIAs)

Where the college plans to adopt a new process, product or service which involves Personal data the college will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures, which demonstrate how we build data protection into our processing activities reducing any risks to individuals (data subjects) and potential reputational damage and fines or penalties. Situations where the college may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

15.1. Large scale and systematic use of personal data for the purposes of automated decision making or profiling where legal or similarly significant decisions are made

15.2. 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

15.3. Systematic monitoring of public areas on a large scale e.g. CCTV cameras

15.4. To identify the most effective method of complying with our data protection obligations and meeting individuals' (data subjects) expectations of privacy

15.5. To ensure all necessary parties are involved from the planning stage of a project e.g. implementation of new systems or a change to the way we process data

15.6. To assess appropriate safeguards are in place where personal data is intended to be transferred outside the EEA. Transfer includes sending personal data outside the EEA – see Transfer out the EEA section.

15.7. To allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to our reputation, which might otherwise occur

15.8. To assess whether new technologies or processing is likely to result in a high risk to the rights and freedoms of individuals (data subjects) or

15.9. To enable the Data Protection Officer to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR

All DPIAs must be reviewed and approved by the Data Protection Officer. All Blackpool Sixth Form College staff will follow the data protection impact assessment (DPIA) procedure and a central register of our data protection impact assessments will be maintained.

16. Data Security

16.1. The college takes information security very seriously and the college will use appropriate technical and organisational measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

17. Data Processors

17.1. When appointing an external data processor, the college will ensure that appropriate contracts are in place.

17.2. Contracts with external organisations must provide 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.

17.3. 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.

18. Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, for example ‘deliberate, unauthorised and unintentional’ incidents.

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:

18.1. **Confidentiality breach** - where there is unauthorised or accidental disclosure of, or access to, personal data e.g. hacking, accessing internal systems to which you are 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 member of staff, student or parent, or disclosing information over the phone to the wrong person.

18.2. **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 backup, or loss of an encryption key.

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

19. Notifying breaches to the ICO

As an organisation we have to report breaches to the Information Commissioner’s Office within 72 hours of detection where the breach is likely to result in a risk to the rights and freedoms of individuals (data subjects). Failure to report a breach when required to do so may result in penalties and fines of up to €20 million, or 4% of an organisation's global turnover.

Notifying breaches to individuals (data subjects) affected	The college will notify the individuals (data subjects) affected by the data breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination. Whilst we are still required to notify the ICO, we are not obliged to notify the individuals (data subjects) affected where:

	● there are technological and organisational protection measures in place (e.g. encryption) ● we have taken action to eliminate the high risk ● it would involve disproportionate effort – in this case individuals (data subjects) must be informed some other way e.g. by a notice in newspapers
Reporting a breach or concern	● Data breach and data concerns within The Blackpool Sixth Form College should be notified to the Data Protection Officer immediately as per the data breach management procedure - see flowchart at Appendix 4 ● Data breach and data concerns from those outside The Blackpool Sixth Form College should be made to the Data Protection Officer– see 'contact section' below ● The college will follow guidance from the ICO where necessary to determine if the breach is reportable ● The college will maintain a register of data breach incidents and concerns

20. Data security

The Blackpool Sixth Form College takes information security very seriously and has security measures against unlawful or unauthorised processing of personal data and against 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 will ensure that the physical security of our buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
The Blackpool Sixth Form College, its employees and others with authorised access to personal data will ensure that appropriate IT and physical data security controls are used to protect unauthorised access to confidential records and personal data.

21. CCTV, videos and photography

The college understands that recording images of identifiable individuals (data subjects) constitutes processing personal information, so it is done in line with data protection principles.

CCTV	The CCTV Policy will be followed in relation to the use and purpose of CCTV monitoring across our various buildings and grounds. The college will also set out the purposes for CCTV monitoring in our privacy notices.

Photographs and non-CCTV recorded images	All may be taken for a variety of purposes, these will be outlined on our privacy notices and the college will normally make it clear as to the purpose at the time the photograph/video is being captured. Where we do not have a legal or contractual basis for taking photographs or recording/videoing of students, staff and others the college will obtain consent from the individual concerned (or person with legal responsibility/legal guardian if under the age of consent or the person is deemed not capable of giving consent).
Images/videos captured by individuals (data subjects) for recreational/ personal purposes	For clarification, images and videos captured by individuals (data subjects) for recreational/personal purposes e.g. by a family member for family use are exempt from the GDPR, however, at times it may be necessary for us to ask you not to take photographs or use recording equipment for instance, events which may involve young children or vulnerable groups.

22. Concerns about your personal information

Concerns in relation to the processing of personal data, or the way your data privacy rights have been handled, can be directed to the Data Protection Officer in the first instance to enable us to investigate the concern(s). The college will aim to carry out the internal review as soon as possible. If you are dissatisfied with our response or if we fail to review your concerns, you have the right to escalate your concern directly to the Information Commissioner's Office (ICO). The ICO provides an online facility for reporting complaints which you will find at https://ico.org.uk/concerns/.

23. Transfer of Data outside the European Economic Area (EEA)

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. The college does not consider that it transfers personal data outside the EEA, or any country where appropriate adequacy measures are not in place. This applies to our own personal data storage, or any company that the college uses that are based overseas or their storage facilities are based overseas.
The college ensures it continually reviews its own processes and the compliance of its partners or contractors to ensure that we would be aware if any data transfers outside the EEA were required.

23.1. There are 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. The college must

consider this when appointing a supplier outside the EEA, or a supplier with group companies outside the EEA, which may give access to the personal data to staff outside the EEA.

23.2. College personnel must not export personal data, inside or outside the EEA, without the approval by the Data Protection Officer.

The Blackpool Sixth Form College does not currently transfer data outside the EEA.

24. Information Commissioner's Office (ICO)

The ICO is the UK's data protection regulator (Lead Supervisory Authority). The Blackpool Sixth Form College is registered as "Data Controller" with the Information Commissioner's Office as follows:
The Blackpool Sixth Form College - Registration No: Z5758025

25. Contact

If you have any feedback about this policy please contact the Data Protection Officer:

By Post: Data Protection Officer
The Blackpool Sixth Form College
Blackpool Old Road
Blackpool
FY3 7LR

or **email:** dpo@blackpoolsixth.ac.uk

26. Other related policies

26.1. Data Retention Policy and Schedule
26.2. Security Policy
26.3. CCTV Policy
26.4. Staff Code of Conduct

Appendix 1.

General data protection guidelines for staff

The majority of staff will process personal data on a regular basis as part of their role in college whether it is prospective, current or former students/employees, contractors, visitors etc.

A large proportion of staff will have access to and process student data in their daily work routine e.g completing registers, marking assessments and recording grades, safeguarding, student support services, writing reports or references, or as part of a pastoral role. The college will ensure through registration procedures that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 2018 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details i.e. name and address
- Details about class attendance
- Coursework marks, grades and associated comments
- Pastoral notes, including matters about behaviour and discipline

Information about a student's physical or mental health, sexual life, political or religious views is sensitive and can only be collected and processed with the students' explicit written consent, usually via the Student Services team, Additional Learning Support team, Examinations team.

Examples:

- keeping of sick notes, medical correspondence outlining conditions and treatments
- recording information about dietary needs, for religious or health reasons, while organising for students to take part in off-site activity
- recording information that a student is pregnant, as part of pastoral duties.

Disclosure of such information without consent is permitted only in "life or death" or safeguarding circumstances, e.g., if a student is unconscious, a teacher can tell medical staff that the student is pregnant or a Jehovah's Witness.

Sensitive information must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a

password-protected computer file. All staff have a duty to make sure that they comply with the data protection principles, as set out in the Data Protection Policy. In particular, staff must ensure that records are:

- accurate
- up-to-date
- fair
- kept securely
- disposed of safely

Staff must not disclose personal data to any other student, parent or other person not in employment at the college without authorisation or agreement from the data controller, or in line with college policy. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with college policy.
The Act requires data to be kept securely in relation to both unauthorised access and loss.

All staff have a duty to maintain data security, in particular by not leaving data accessible in an unlocked office, filing cabinet or personal bags. Computer screens should not be placed where they could be easily seen by unauthorised people. Computers should be locked when left unattended. (Contact the Tech Support team for guidance about this, if necessary.)
Electronic transfer of personal data cannot be considered secure. Using email or fax to transmit personal data should be treated with extreme caution. This is particularly important when sending confidential documents, such as references, to third parties outside college. Sending password documents in password protected files should be the minimum level of security applied.
Before processing any personal data, all staff should consider the checklist below.

Staff checklist for recording data:

- Do you really need to record the information?
- Is the information ‘standard’ or is it ‘sensitive’(special category)?
- If it is sensitive, do you have the data subject’s express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- iIf yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Appendix 2.
Glossary/Definitions of main terms

College	The Blackpool Sixth Form College
Data	Any information which will be processed and stored. This can be written, taped, biometric, film, photographic or other information
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 such as trade union membership, health data, genetic data and religious beliefs. These more sensitive types of data are called “Special Categories of personal data” and are defined below. Special Categories of personal data are given extra protection by Data Protection Laws.
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 (including learning difficulties or disabilities), sexual life or sexual orientation and criminal convictions. Special categories of personal data are subject to additional controls in comparison to ordinary personal data.
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.
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 the 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 involve access to or use of personal data. College examples include software support we receive for our college safeguarding software, which contains personal data, and outsourcing of financial processes such as salaries to ‘Cintra’ where we define the purpose and the processing requirements involved.

Data Protection Officer	Member of staff designated by the college to ensure compliance with data protection policies and procedures.
Data processing	Recording, accessing, altering, adding to, changing, disclosing or merging any data.
Data protection principles	The underlying principles that determine what data can be collected, processed and stored.
EEA	The EEA comprises of the following countries: 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.
Information Commissioner Office	The UK's data protection regulator, and the Commissioner is an officer appointed by the State to administer the provisions of the Data Protection Act.
Individuals (data subjects)	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 our personal/ business partners and employers.
Notification	The process of informing the Information Commissioner that an organisation or individual will be processing personal data other than for private use.
Subject consent	Before processing personal data the agreement of the individual must be obtained.
Data Protection Laws	The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Appendix 3.

Data breach procedure

Every care is taken by the college to protect personal data from situations where a data protection breach could compromise security.

This policy and procedure applies to all staff, students, personal/ business partners, Directors, employers, suppliers or third parties we work with. It should be read in conjunction with the college's Data Protection Policy.
The objective of this procedure is to enable staff to act promptly to contain any breaches that occur and minimise the risk associated with the breach and to take action if necessary to secure personal data and prevent further breaches.

The college expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of college business and must take appropriate steps to safeguard this information.

Under the Data Protection Act, although there is no legal obligation on data controllers to report breaches of security, the new General Data Protection Regulation (GDPR) means we have to report any breach that is likely to impact on data subjects. The procedure below is set out to help you identify when a breach has taken place and what the action should be.

What is a data breach?
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the purposes of the colleges business.
A breach in IT security or an external threat to college networks or systems should also be documented and investigated in the same way.

A personal data breach includes, but is not restricted to, the following:

- Loss or theft of data or equipment on which personal or sensitive data is stored (i.e. loss of laptop, USB pen, iPad/Tablet device, or paper record)
- Inappropriate access controls allowing unauthorised use
- Equipment theft or failure
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Human error
- Offences where information is obtained by deceiving the holder of the information, the college
- Unauthorised disclosure of sensitive/personal data

Destruction of paperwork or electronic records in accordance with the internal retention

schedule does not constitute a breach.

Definition of personal data:
Can a living individual be identified from the data, or from the data and other information in your possession? If the data 'relates to' the identifiable living individual, whether in personal or family life, business or profession, then it is **personal data**.

We collect **personal data from students on their application and enrolment forms**, which we then input into the college student database. This includes information such as their name, contact details, date of birth, parent/guardian or emergency contact, ethnicity, learning difficulties and disabilities, health information, criminal convictions (if applicable), and their photo (for their membership card). We may also collect financial details if the student is in receipt of a bursary, uses the online ParentPay payment portal to pay for trips, (this could also be parent/guardian financial details if they pay for the trips).
The information we record whilst the learner is studying with us is also considered personal data, used to monitor their progression, attendance, behaviour, target grades, assessments, and any support that is needed. College staff also use students personal data every day in registers and classlists.

We collect **personal data from staff as they complete the recruitment process** and in relation to their employment contracts. Each staff member will have an employee file on paper and an electronic record held on our central HR system. This includes information such as their name, contact details, date of birth, NI number, next of kin, bank details, pension details, certifications/qualifications, employment terms and conditions. The college also records information relating to performance, training, sickness absence and any incidents or disciplinary action that have occured during their employment.

We hold **personal and financial information about our Directors, employers, suppliers and third party organisations**. Although the amount of information we hold on individuals may be minimal, and may relate to their business or profession, if they are identifiable as a living individual it still counts as personal data.
The information we collect may be on paper, stored in electronic files or stored within systems, but all formats constitute part of the individual's personal data, and as such must all be protected by college employees against a breach occurring.

How will the college assess the risk
Some data breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role. Following immediate containment, the risks must be assessed which may be associated with the breach, potential adverse consequences to the individuals, as well as, the college itself, and the seriousness of the breach must be considered, further to immediate containment
Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the college is able to quickly identify the classification of the data and assess the risk to data subjects or the college.
For the purposes of this policy data security breaches include both confirmed and suspected incidents.

The following must be considered upon discovering a data breach:

- the type of data involved
- its sensitivity
- if data has been lost or stolen, whether data has been protected by encrypted devices or software
- what has happened to the data, such as the possibility that it may be used to cause harm to the individual(s)
- who the individuals are, number of individuals involved and the potential effects to those data subject(s)
- whether there are wider consequences to the breach
- whether any actions have been taken during the breach that contravene the policies, procedures and training in place.

What do you do if you discover a data breach?

The first thing to do is NOT to panic. If you have discovered a breach and you follow the procedure you are already taking control of the situation and playing your part in reporting the breach.

To ignore a possible data breach or fail to follow the correct procedure may result in disciplinary action.

Step 1

Identifying and reporting a data breach

If you discover a data breach, you must report this to our **Data Protection Officer (DPO)** immediately. Any breach, or suspected breach, can be sent for their attention on dpa@blackpoolsixth.ac.uk.

All breaches big or small, regardless of the harm or potential harm, should be identified and reported.

False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable the college to learn lessons in how to respond and the remedial action that we put in place.

We have a legal obligation to keep a register of all data breaches. Please ensure that you report any breach, even if you are unsure whether or not it is a breach.

When a data breach is reported to the college DPO, they will promptly investigate the breach to ascertain whether we are fully aware that a breach has occurred leading to personal data being compromised for our data subjects.

The investigation will be done within 48 hours of a breach being reported to the college, so that it can ensure it complies with the 72 hour deadline to report any data subject or serious security breaches in a timely way to the ICO.

A data breach may result in disciplinary action.

Once a data breach is reported the following procedure will be invoked.

Step 2

Assessing a data breach

Once a data breach has been reported and the Data Protection Officer (DPO) has conducted an initial investigation and has decided that a breach has occurred, the DPO will log the breach and will carry out an initial assessment of the breach to evaluate its severity.

The DPO and Senior Leadership Team (SLT) will investigate the breach and consider any on-going risks to any individuals affected and formulate a recovery plan, if required, to minimise further the risk. SLT will also consider any on-going risks to the college, the impact on the college reputation and the effect it may have.

As part of the recovery plan, our DPO and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

Step 3

Notifying a breach to the Information Commissioner's Office (ICO)

Unless the breach is unlikely to impact on data subjects or result in a risk to the rights and freedoms of individuals, the college must notify the breach to the ICO within 72 hours of becoming aware of the breach. The college must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.
The content of the notification will be drafted by our DPO, and any notification to the ICO must only be made by the DPO.

Step 4

Notifying a breach to other relevant 3rd parties

We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include insurers, police, employees, parents/guardians, banks as examples.

The decision as to whether any third parties need to be notified will be made by our DPO and SLT. They will decide on the content of such notifications and act within 5 days of becoming aware of the data breach.

Appendix 4.

Confidential Waste Procedures

Purpose

Confidential waste can be broadly defined as resources containing information about college business with a selected readership and where disclosure may compromise personal privacy, financial or strategic information and therefore must be disposed of responsibly.

These procedures underpin the requirements of disposal of data in the Data Protection Policy and it is a condition of employment that employees will abide by the rules and policies made by the college. Any failure to follow the policy can therefore result in disciplinary proceedings.

Confidential waste covers resources containing personal and business sensitive data such as paper files, photographs, carbonised inserts and printing films, floppy discs, CDs, DVDs and memory sticks. Below is a non-exhaustive list of documents that would be classified as being confidential in nature. Please note that this list is not exhaustive, and is intended to provide guidance only.

Records or information that contains personal information about a living individual for example:

- Staff personnel records
- Staff or student discipline or appeal records
- Student records
- Exam papers
- Job applications
- Interview notes
- References
- Admissions records
- Redundancy records
- Sick pay records
- Maternity pay records
- Income tax and National Insurance returns
- Wages and salary records
- Accident books and records
- Health records
- Budget Information/Invoices
- Meetings minutes
- Medical records
- Questionnaire or other data collected under an understanding of confidentiality
- Other letters or documentation which pass comment on a named living person
- Correspondence or other documents that reveal the contact details or any financial details of a named living individual

Any record which, if made public before a certain period, may breach commercial confidentiality for example:

- Contracts
- Tenders
- Purchasing records
- Maintenance records
- Insurance records
- Unpublished accounting records

Disposal Responsibilities and Arrangements

Paper confidential items, which are scheduled for destruction, must be disposed of in the following appropriate ways:

1. Shredded and then placed in the waste paper recycling collection bins around college.
2. Placed in secure (locked) confidential waste bins located in the Principalship, Finance and MIS offices.
3. Placed in clearly labelled confidential waste bags for removal by the Estates team to a secure storage location.

Staff are responsible for ensuring Estates are alerted to collection requirements for disposal option 3 with sufficient notice. Bags with confidential waste are not to be left in offices overnight, or any extended period over weekends or holiday periods as they present a risk to data protection compliance.

Disposal of waste via options 2 and 3 will be administered by the Estates Department via a commercial confidential waste arrangement.

For all other types of confidential waste requiring secure disposal please contact the Estates team directly for instruction.