Bury College Policy and Procedures

Appropriate Policy Document

1. About this Policy

The Appropriate Policy Document (APD) provides information about the lawful basis and safeguards Bury College (the College) has in place to process Special Category and Criminal Offence Data. This is to satisfy some of the conditions for using such data in Schedule 1, Part 4 of the UK Data Protection Act 2018 (DPA), which require the organisation as the controller to set out and explain the procedures for securing compliance.

The APD also complements the Data Protection Policy.

2. PERSONAL DATA PROCESSED

2.1 The College processes the following Special Category Data:

a) Information about race or ethnicity, religious beliefs.
b) Information about health and wellbeing, including any medical condition; health, sickness and safety records, sickness absence, occupational health interactions and disability information, including mental health.
c) Information relating to maternity, paternity, shared parental or adoption leave.

2.2 The College also processes Criminal Offence Data, which is information about any relevant criminal convictions and offences.

3. CONDITIONS FOR PROCESSING

3.1 Processing Special Category Data

a) UK GDPR, Article 9(2)(a) – explicit consent. This could apply to gather information about your race, ethnicity and religious beliefs.
b) UK GDPR, Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by UK law on to the College or the data subject in connection with employment, social security, or social protection. For examples where the College processes staff sickness and absences information. Further condition for the lawful use of this data is in the DPA, Schedule 1, Part 1, paragraph 1 – employment, social security and social protection.
c) UK GDPR, Article 9(2)(c) – where processing is necessary to protect vital interests. An example of this processing would be using health information about a member of staff or learner in a medical emergency.
d) UK GDPR, Article 9(2)(f) – for the establishment, exercise, or defence of legal claims. Examples of this processing include processing relating to any employment tribunal or other litigation.

3.2 Processing Criminal Offence Data

a) UK GDPR, Article 10 – as authorised by UK law. This is only applicable to certain roles. Further condition for the lawful use of this data is in the DPA, Schedule 1, Part 1, paragraph 1 – employment, social security and social protection.

4. MEASURES FOR ENSURING COMPLIANCE WITH PRINCIPLES

4.1 Accountability principle

1. In accordance with the accountability principle, the College maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. The College will carry out data protection impact assessments (where appropriate) in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and default.

2. The College follows the data protection principles set out in Article 5 of the UK GDPR, and Part 2 of the DPA 2018 for processing, as follows:
   a) The appointment of a data protection officer who reports directly to the highest management level.
   b) Taking a 'data protection by design and default' approach.
   c) Maintaining documentation of processing activities.
   d) Adopting and implementing data protection policies.
   e) Implementing contracts with data processors.
   f) Implementing appropriate security measures in relation to the personal data.
   g) Carrying out data protection impact assessments (where required).
   h) Regular review of accountability measures.

4.2 Compliance with the data protection principles

1. Principle (a): lawfulness, fairness and transparency
   a) The College provides clear and transparent information about the processing of personal data including the lawful basis for that processing in the College's Records of Processing Activities (ROPA), Privacy Statement and this policy document.

2. Principle (b): purpose limitation
   a) The College process personal data as necessary to provide services and, if appropriate, following a controller's specific instructions.
   b) The College shall not process personal data for purposes incompatible with the original purpose it was collected for.
   c) Where the College is required to share personal data with the third party, The College will complete any necessary due diligence checks, such as

vendor assessments, data protection impact assessment, or complete data sharing agreements.

3. Principle (c): data minimisation
   a) The College shall collect personal data necessary for the relevant purposes and ensure it is not excessive. The information processed is necessary for and proportionate.
   b) Where personal data is provided to The College or obtained but is not relevant to our stated purposes, it will be erased.

4. Principle (d): accuracy
   a) The College shall ensure that where personal data is identified as inaccurate or out of date, having regard to the purpose for which it is being processed, and the College will take every reasonable step to ensure that data is erased or rectified without delay. If the College decides not to either erase or rectify it, for example because the lawful basis means those rights don't apply, the decision will be documented.

5. Principle (e): storage limitation
   a) All Special Category Data processed by the College for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for specific periods. These are reviewed regularly and updated when necessary.

6. Principle (f): integrity and confidentiality (security)
   a) The College ensures that electronic information is processed within secure networks. Hard copy information is processed in line with our security procedures. The systems used to process personal data allow data to be erase or updated as required. Electronic systems and physical storage have appropriate access controls applied, such as two-factor authentication.