Data Protection Policy

Policy Statement

Wigan & Leigh College aims to comply with the Data Protection Principles and as such will process any data held fairly and lawfully. The College will ensure data is held securely and that safe processes are employed when dealing with data.

The legal basis for this policy is compliance with the Data Protection Act 2018. The Act writes into English law the European Union's General Data Protection Regulation (GDPR).

Statement of Principles

The organisation needs to keep certain information about its employees, customers and other users of its facilities to allow it to monitor performance, achievements, health and safety and other statutory requirements. It also needs to process information so that staff can be recruited and paid, and legal obligations to funding bodies and the government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the organisation must comply with the Data Protection Principles, which are set out in the Data Protection Act 2018. In summary, these state that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and where necessary kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Important Note: The Data Protection Act 2018 extends the scope of legislation to include *written and printed etc. material*, not just the electronic data which was covered by earlier enactments.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, this Data Protection Policy is in place.

Status of the Policy

This policy is incorporated in the formal contract of employment. Infringement of the requirements of this policy may result in disciplinary action being taken. For the purposes of this document, reference to "employee" or "member of staff" includes any person carrying out work as a contractor, consultant or in a similar role.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter initially with the designated data controller. If the matter is not resolved it should be raised as a formal grievance.

Responsibilities and Duties

All staff are responsible for:

- Checking that any information that they provide in connection with their employment is accurate and up to date.
- Informing the organisation of any changes to information which they have provided, e.g. changes of address.
- Informing of any errors or changes in staff information.

If and when, as part of their responsibilities, staff collect information (e.g. personal information, opinions about ability, or details of personal circumstances) about other people, whether employees or people outside the organisation, they must comply with any guidelines which may be published. In particular, they must seek the permission of the data controller for their proposed information collection and uses.

Data Security – all staff are responsible for ensuring that:

- Any personal data, which they hold, or for which they are responsible, is kept securely, for example:
  - Kept in a locked filing cabinet; or
  - In a locked drawer;
  - If it is computerised, then the computer itself is kept in suitably secure conditions. Data should not be stored on the hard drives of desktop and personal computers but on the networked storage facilities provided.
  - Where it is necessary to store information on laptop computers (or off-site) then the machine must at all times be maintained physically secure. Where the data is particularly sensitive, consideration must be given to the adoption of additional security measures which would protect the information in the event of the loss or theft of the computer – i.e. encryption. Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise.
  - Data that is held on mobile devices must be password protected and where personal or sensitive data must be encrypted.
  - Where information is to be gathered through, or used on, a website, then appropriate measures must be in place to control access and prevent unauthorised disclosure.

- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Advice on the collection, retention and secure storage of information may be obtained from the data controller.

Dealing with Potential Breaches of the Data Protection Policy

- All security breaches must be reported to the Data Protection Officer immediately.
- The Data Protection Officer will inform the individual(s) to whom the personal data relates that there has been a potential breach.
- The Data Protection Officer will then conduct an investigation to establish the extent and seriousness of the alleged breach.
- The Data Protection Officer will prepare a report on the potential breach for submission to the Principal, with recommendations for further action, if appropriate.
- The Information Commissioner's Office will be informed, if appropriate.
- Disciplinary action may be taken against members of staff or students for any such breach of data protection, under the relevant College policy.

Staff should note that unauthorised disclosure is a breach of the Data Protection Act and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

The Executive have overall responsibility for monitoring the steps taken in their area of management responsibility to ensure that the Act and this Policy are complied with. Particular care must be taken when work is being undertaken externally or when an existing body of material is being brought in for the first time.

Implementation

Rights to Access Information

Employees and other users have the right to access any personal data that is kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the Data Controller.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 month from the receipt of the request.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

The College has a duty of care to all staff and must therefore make sure that employees and those who use the college facilities do not pose a threat or danger to other users.

Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made.

Processing Sensitive Information

Sometimes it is necessary to process sensitive information about a person such as race, gender or family details. This is done to ensure the College can operate policies on matters such as sick pay or equal opportunities. The College may also ask for information about particular health needs or disabilities. The College will only use such information in the protection of the health and safety of the individual, but will consent to process information, for example, in the event of a medical emergency. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for the College to do this.

Sensitive Information and the PREVENT Duty

The Counter Terrorism and Security Act 2015 states that its provisions do not "require or authorise the making of a disclosure that would contravene the Data Protection Act 2018" or "a disclosure of any sensitive information."
Under the Data Protection Act particular protections are given to the processing of "sensitive data," which includes information on ethnic background, political opinions and religious beliefs.
However, subsequent legislation has set out exemptions to these general rules, most notably when processing "is necessary for the purposes of the prevention or detection of any unlawful act."

The Data Controller and the Designated Data Controller

The College as a public body is the data controller under the Act, and the Executive is therefore ultimately responsible for implementation. However, the designated data controller will deal with the implementation of agreed policy and day to day matters.

The College has a designated data controller. This is the Assistant Principal, College IT Systems and MIS, and his absence, the IT Manager may be consulted.

Retention of Data

The College will keep some forms of information for longer than others to comply with funding, freedom of information and audit requirements.

The College will need to keep central personnel records indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

In due course retention periods and policies for all classes of document will be determined and codified in the Record Management Procedure being created as part of the work necessary to discharge the agency's responsibilities under the Freedom of Information Act.

Compliance

Compliance with the Data Protection Act 2018 is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to the College facilities being withdrawn, or even a criminal

prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the data controller.

Monitoring Arrangements

This Policy will be monitored and reviewed by Principal, and annual reports will be received by the Executive Team and the Resources Committee of the Governing Board.

Signed		College Principal
Originator	Dave Harrison	Assistant Principal College IT Systems & MIS
Version	3.0	
Date of Issue	March 2021	

Review Date March 2024

Copies of all approved College Policies can be found on the Staff Intranet.