



Issue Date: March 2023

Review Cycle (Years): Annually

Next Review Date: 29th March 2024

Person Responsible: Data Protection Officer

DATA PROTECTION POLICY

APPROVAL/CONSULTATION REQUIREMENTS

WHO BY	REQ?	DATE	WHO BY	REQ?	DATE
SLT	Y <input checked="" type="checkbox"/>	06-03-23	Corporation	Y <input checked="" type="checkbox"/>	29-03-23
Health-Safety Comm.	Y <input type="checkbox"/>		Finance-Resources Comm.	Y <input checked="" type="checkbox"/>	16-03-23
Trades Union	Y <input type="checkbox"/>		Audit Comm.	Y <input type="checkbox"/>	
Education-Standards Comm.	Y <input type="checkbox"/>		Remuneration Comm.	Y <input type="checkbox"/>	

POLICY LOCATION: Internal ☒ (**Sharepoint**) External ☒ (**Website**)

Related Documents: • IT Acceptable Use Policy

1. INTRODUCTION

- 1.1 Coventry College needs to collect and process substantial volumes of personal data in order to carry out its core functions and activities. The College is the Data Controller for most of the personal data it processes and is committed to full compliance with applicable data protection legislation. This includes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (referred to as the General Data Protection Regulation or “**GDPR**”) and all legislation enacted in the UK in respect of the protection of personal data, including The Data Protection Act (2018) as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- 1.2 This Policy should be read in conjunction with the College’s IT Acceptable Use Policy and related Procedures and Codes of Practice. These provide more detailed guidance on the correct handling of personal data and together with this policy are an integral part of the overall information governance framework of the College.
- 1.3 The College has appointed a Data Protection Officer who is responsible for informing and advising the College and its employees on its data protection obligations, and for monitoring compliance with those obligations and with the College’s policies.

2. PURPOSE AND SCOPE

- 2.1 All College employees, students and other authorised third parties (including temporary and agency workers, contractors, interns and volunteers) who have access to process any personal data held by or on behalf of the College, must adhere to this policy and associated Procedures and Codes of Practice.
- 2.2 The term ‘Personal data’ refers to any information relating to an identified or identifiable living person (referred to as a ‘data subject’); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This policy is therefore applicable to, but not limited to, the personal data of all

members of the public, applicants, students, employees, governors and other stakeholders whose personal data is processed by the College.

- 2.3 The information covered by the policy includes all written, spoken (recorded) and electronic personal data held, used or transmitted by or on behalf of the College, in whatever media. This includes personal data held on computer systems, hand-held devices, phones, paper records, and personal data transmitted and recorded orally.
- 2.4 Third parties engaged by the College to act as Data Processors will be required to confirm their compliance with all aspects of this Policy.

3. GOVERNANCE

3.1 The Data Controller

Coventry College as a corporate body is the data controller, and the Corporation is ultimately responsible for the implementation of all appropriate policies and procedures to meet its obligations. Governors, employees, agency workers, contractors and consultants of the College are required to implement the Policy on behalf of the College and are referred to throughout this document as 'Employees'.

3.2 The Data Protection Officer

As required by all Public Bodies, the College has appointed a Data Protection Officer to oversee all aspects of this Policy and associated Procedures and Codes of Practice. Details of their name and contact details will be published on the College website as well as being widely available to all staff and students across the College.

3.3 The Strategic Lead for Data Protection and Department Co-ordinators

In addition, the College has assigned responsibility for day to day oversight of Data Protection to oversee data protection for the College. These roles support the effective implementation of policy, procedure and codes of practice with all staff, ensuring that there is a strong local focus across the large physical and organisational scope of the College's activities.

- 3.4 In discharging their duties, the Data Protection Officer will have a direct line of reporting through the Secretary to the Corporation to the Finance & Resources Committee of the Corporation Board. A Data Protection report will be presented annually to the Finance & Resources Committee.

- 3.5 The implementation of the Data Protection Policy is continuously monitored by the Data Protection Officer.

4. DATA PROTECTION PRINCIPLES

- 4.1 When using Personal Data, Data Protection Laws require that the College complies with and demonstrates compliance with the following principles. These principles require the College to ensure that:

- 4.1.1 We will process personal data lawfully, fairly and in a transparent manner;

- 4.1.2 We will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

- 4.1.3 We will only process the personal data that is adequate, relevant, and necessary;
- 4.1.4 We will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
- 4.1.5 We will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and
- 4.1.6 We will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, accidental loss, destruction, or damage

5. BASIS FOR PROCESSING PERSONAL DATA

- 5.1 In relation to any processing activity that involves personal data we will, before the processing starts for the first time and then regularly while it continues:
 - 5.1.1 Review the purposes of the processing activity, and select the most appropriate lawful basis for that processing, i.e. That the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract;
 - 5.1.2 That the processing is necessary for compliance with a legal obligation to which the College is subject;
 - 5.1.3 That the processing is necessary for the protection of the vital interests of the data subject or another natural person;
 - 5.1.4 That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the College;
 - 5.1.5 Where the College is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of the College or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject; or
 - 5.1.6 That the data subject has consented to the processing.
 - 5.1.7 Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose);
 - 5.1.8 Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
 - 5.1.9 Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices; and
 - 5.1.10 Where sensitive personal data is processed, also identify a lawful special condition for processing that information (see paragraph 6 below), and document it.

6. SENSITIVE PERSONAL DATA

- 6.1 Sensitive Personal Data (sometimes referred to as 'special categories of personal data') are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
- 6.2 The College may from time to time need to process sensitive personal data. We will only process sensitive personal data if:
- 6.2.1 We have a lawful basis for doing so as set out in paragraph 5.1.1 above. One of the special conditions for processing sensitive personal data applies:
- a) The data subject has given explicit consent;
 - b) The processing is necessary for the purposes of exercising the employment law rights or obligations of the College or of the data subject;
 - c) The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
 - d) The processing relates to personal data which are manifestly made public by the data subject;
 - e) The processing is necessary for the establishment, exercise or defence of legal claims; or
 - f) The processing is necessary for reasons of substantial public interest.
- 6.3 The College's privacy notices for different Colleges of data subjects set out the types of sensitive personal data that the College processes, what it is used for and the lawful basis for the processing.

7. IMAGES AND RECORDINGS

- 7.1 Where the College collects images and/or recordings and individuals may be identified in those images, arrangements for collection, storage and disposal will be carefully considered based on the basis for processing. In some cases, arrangements for example for the security or sharing of media, may differ from standard procedures. In particular, the College will;
- 7.1.1 Ensure that all images of students and members of the public collected for marketing and communications purposes are supported by clear and informed consent, which may be amended or withdrawn by the individual at any time. The College will ensure that individuals are aware of the limitations of their right to restrict processing in relation to images already published in digital or paper form and will involve individuals in the approval process for any use of their image which might have a significant public reach or impact.
- 7.1.2 Ensure that CCTV images and recordings are collected, stored and used within a secure environment, in accordance with the published procedures and codes of conduct.
- 7.1.3 Use images and recordings created as part of the teaching, learning and assessment process will only be used to provide access and support to students as part of their learning programme. This may include the recording of lessons

and other activities, which may include images of teachers, students and other employees. Such images and recordings will be shared with staff and students via the agreed Digital Learning Platform(s) and therefore subject to specific, more open arrangements for security and retention.

- 7.1.4 Images and recordings of employees, created for the purposes of delivering teaching, learning and assessment through online platforms, or to create reusable teaching and learning resources, will be separately classified and subject to specific criteria for retention and re-use.

8. DATA PROTECTION IMPACT ASSESSMENTS

- 8.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the College is planning to use a new form of technology), we will, before commencing the processing, carry out a Data Protection Impact Assessment (DPIA) to assess:
 - 8.1.1 Whether the processing is necessary and proportionate in relation to its purpose;
 - 8.1.2 The risks to individuals; and
 - 8.1.3 What measures can be put in place to address those risks and protect personal data.
- 8.2 The DPIA must be completed according to the College's Data Protection Impact Assessment Procedure, reviewed by the Data Protection Officer, and approved by a member of the Executive Leadership Team before any changes to process are implemented.
- 8.3 Where a DPIA reveals risks which are not fully mitigated, the College will review the assessment, and if required, the Information Commissioners Office (ICO) must be consulted for further advice. The Data Protection Officer will be responsible for all consultation required with the ICO.

9. DOCUMENTATION AND RECORDS

- 9.1 We will keep written records of processing activities
- 9.2 We will conduct regular reviews of the personal data we process and update our documentation accordingly. This may include:
 - 9.2.1 Carrying out information audits to find out what personal data the College holds;
 - 9.2.2 Distributing questionnaires and talking to staff across the College to get a more complete picture of our processing activities; and
 - 9.2.3 Reviewing our policies, procedures, contracts, and agreements to address areas such as retention, security and data sharing.
- 9.3 We will maintain a single central record of all personal data breaches and subject access requests in order to ensure full compliance with our procedures and to allow for regular review and improvement planning in areas of high risk or poor compliance.

10. PRIVACY NOTICES

- 10.1 The College will publish Privacy Notices relating to all Colleges of data subject, informing the people from whom we collect information about the personal data that we collect and hold relating to them, how they can expect their personal data to be used and for what purposes.
- 10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.
- 10.3 Individuals will be signposted to the appropriate privacy notice(s) on the College website(s) whenever new or additional personal data is collected or amended in the course of our usual activities. Privacy Notices will be made public and accessible to all individuals via the College website.

11. INDIVIDUAL RIGHTS

11.1 Data subjects have the following rights in relation to their personal data:

- 11.1.1 To be informed about how, why and on what basis that data is processed. At the College, we customarily do that via privacy notices;
 - 11.1.2 To obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request;
 - 11.1.3 To have data corrected if it is inaccurate or incomplete;
 - 11.1.4 To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
 - 11.1.5 To restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where the College no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim; and
 - 11.1.6 To restrict the processing of personal data temporarily where the data subject does not think it is accurate, or where the data subject has objected to the processing.
- 11.2 Each of the College's Privacy Notices provides details of how these individual rights can be exercised.
- 11.3 All Subject Access Requests will be directed by Staff to the Data Protection Officer who will ensure that the agreed procedure is followed to establish the identity of the individual, the scope of their request, and the timely provision of a response.
- 11.4 The College will not charge a fee for the processing of a Subject Access Request but reserves the right to pass on the cost of providing additional or repeat copies of the same information, as well as the cost of meeting any manifestly unfounded or excessive requests.
- 11.5 In respect of the Right of Erasure (Right to be Forgotten), this is a limited right for Individuals to request the erasure of Personal Data concerning them where the use of the Personal Data is no longer necessary; their consent is withdrawn and there is no other

legal ground for the processing; the individual objects to the processing and there are no overriding legitimate grounds for the processing; the Personal Data has been unlawfully processed; or the Personal Data has to be erased for compliance with a legal obligation.

- 11.6 The College will respond to all requests for data erasure within 30 days and will confirm what categories of personal data have been erased, as well as any categories of data retained where they do not fall within the scope of this right.
- 11.7 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 will be erased, or if also retained for another legitimate reason, clearly annotated to prevent future use for marketing purposes.
- 11.8 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format, where the processing is based on consent or on a contract; and the processing is carried out by automated means. This right isn't the same as subject access and is intended to give Individuals a subset of their data. The College will respond to all requests to provide portable data within 30 days, providing either a suitable dataset for transport, or a detailed explanation as to why the request cannot be fulfilled.
- 11.9 Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.
- 11.10 The College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance. The Data Protection Officer will investigate any cases where an individual feels that their rights, including to the rectification of incorrect information or the restriction of use, have not been met.

12. MARKETING AND CONSENT

- 12.1 The College will sometimes contact Individuals to send them marketing materials or to promote the Colleges and other activities of the College. Where the College carries out any marketing, activities will be carefully planned to ensure compliance with Data Protection Law, other applicable legal and regulatory frameworks.
- 12.2 For Marketing activities, consisting of any advertising or marketing communication that is directed to particular Individuals and using their personal information, the College will operate within a framework of consent, and maintain records within its central systems for Student Records and Customer Relationship Management.
- 12.3 For electronic marketing, the College will provide a clear and simple opt-in system for Individuals, and simple means to withdraw consent at any time.
- 12.4 Where information is collected face to face or by telephone, and as part of a specific marketing activity, the College will use a 'soft opt-in' record of consent and provide the individual with a simple opportunity to opt out on all occasions that the information is used.

13. AUTOMATED DECISION MAKING AND PROFILING

- 13.1 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If

employees therefore wish to carry out any Automated Decision Making or Profiling, they must inform the Data Protection Officer who will co-ordinate the completion of a comprehensive DPIA to evaluate the risks associated with the proposed processing activities. Employees must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

14. DATA QUALITY

- 14.1 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 it holds is accurate and kept up to date.
- 14.2 All employees that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.
- 14.3 All employees that obtain personal data from sources outside the College shall take reasonable steps to ensure that the personal data is received has been recorded accurately, is up to date and is limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require employees to independently check the personal data obtained.
- 14.4 In order to maintain the quality of personal data, all employees that access personal data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g., for legal reasons or that which is relevant to an investigation).
- 14.5 The College recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws and makes leaders and managers responsible for data procedures accountable for the maintenance of these principles.

15. INDIVIDUAL OBLIGATIONS

- 15.1 All individuals, including employees, students and members of the public who have provided information to the College are responsible for helping the College keep their personal data up to date. Individuals should let the College know if the information they have provided changes (for example if one moves house or changes details of the bank or building society account to which they are paid).
- 15.2 Employees may have access to the personal data of other employees, students and other clients and suppliers of the College during their employment or engagement. If so, the College expects such members of staff to help meet the College's data protection obligations to those individuals at all times, using information only for the purposes for which it was collected.
- 15.3 If one has access to College personal data, they must:
 - 15.3.1 Only access the personal data that they have authority to access, and only for authorised purposes;

- 15.3.2 Only allow others to access personal data if they are able to verify the identity of the individual and can confirm that they have appropriate authorisation to do so;
- 15.3.4 Not remove personal data, or devices containing personal data (or which can be used to access it), from the College's premises unless appropriate security measures are in place (such as encryption) to secure the information and the device; and
- 15.3.5 Not store personal data on local drives or on personal devices that are used for work purposes.
- 15.4 The College's Data Protection Officer should be contacted if one is concerned or suspects that one of the following has taken place (or is taking place or is likely to take place):
 - 15.4.1 Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal data:
 - 15.4.2 Access to personal data without the proper authorisation;
 - 15.4.3 Personal data not kept or deleted securely; Removal of personal data, or device containing personal data (or which
 - 15.4.4 Can be used to access it), from the College's premises without appropriate security measures being in place;
 - 15.4.5 Any other breach of this Policy or of any of the data protection principles set out in paragraph 4 above.

16. INFORMATION SECURITY

- 16.1 The College will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
 - 16.1.1 Ensuring that, where possible, personal data is encrypted;
 - 16.1.2 Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 16.1.3 Ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and
 - 16.1.4 A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for assuring the security of the processing.
- 16.2 Where the College uses external organisations to process personal data on its behalf, additional security arrangements will be implemented in contracts with those organisations to safeguard the security of personal data. Contracts with external organisations must provide that:
 - 16.2.1 The organisation may act only on the written instructions of the College;
 - 16.2.2 Those processing the data are subject to a duty of confidence;
 - 16.2.3 Appropriate measures are taken to ensure the security of processing;

- 16.2.4 Sub-contractors are only engaged with the prior consent of the College and under a written contract;
 - 16.2.5 The organisation will assist the College in providing subject access and allowing individuals to exercise their rights in relation to data protection;
 - 16.2.6 The organisation will assist the College in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
 - 16.2.7 The organisation will delete or return all personal data to the College as requested at the end of the contract; and
 - 16.2.8 The organisation will provide the College with whatever information it reasonably needs to ensure that they are both meeting their data protection obligations.
- 16.3 Prior to any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant member of staff must seek approval of its terms by the College's Data Protection Officer or one of the College's lawyers.

17. STORAGE AND RETENTION OF PERSONAL DATA

- 17.1 Personal Data (and sensitive personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.
- 17.2 When setting retention periods, consideration will be given to the following key factors:
 - 17.2.1 The purpose for which the data was obtained;
 - 17.2.3 Any specific consents provided by the data subject in relation to the use or retention of that data;
 - 17.2.3 Whether the original purpose has been fulfilled; and
 - 17.2.4 Whether the data needs to be retained to support any potential legal process
- 17.3 Where there is any uncertainty with respect to data retention, employees should consult the College's Data Protection Officer.
- 17.4 The College has a legal responsibility not to keep personal data for longer than needed for the specific purposes agreed when it was collected. At the end of the agreed period for each type of information, also referred to as an Information Asset, the College will take steps to delete such information from its information systems, databases and electronic files, and to destroy paper records using agreed, secure processes.
- 17.5 The retention period of Employee/Personnel Records, Payroll Documentation, Student Records, Statutory Record and Purchase Invoices and Supplier Documentation is listed in Appendix 1 of this document.

18. DATA BREACHES

- 18.1 A data breach may take many different forms, for example:

- 18.1.1 Loss or theft of data or equipment on which personal data is stored;
 - 18.1.2 Unauthorised access to or use of personal data either by a member of staff or third party;
 - 18.1.3 Loss of data resulting from an equipment or systems (including hardware and software) failure;
 - 18.1.4 Human error, such as accidental deletion or alteration of data;
 - 18.1.5 Unforeseen circumstances, such as a fire or flood;
 - 18.1.6 Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
 - 18.1.7 Blagging' offences, where information is obtained by deceiving the organisation which holds it.
- 18.2 If anyone believes personal data held by the College has been compromised in some way they must report this immediately to the Data Protection Strategic Lead or the Data Protection Officer using the standard form provided on the College Intranet.
- 18.3 The College will:
- 18.3.1 Investigate any reported actual or suspected data security breach, making a record of the breach, the steps taken to investigate its possible impact, and the subsequent risk assessment and actions;
 - 18.3.2 Where applicable, make the required report of a data breach to the Information Commissioner's Office without undue delay and within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
 - 18.3.3 Notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law
- 18.4 Any high-risk breach of data protection procedures, which must be reported to the ICO immediately upon discovery, will be reported in parallel to the Principal and Chief Executive or the Chief Finance and Operating Officer by the Data Protection Officer.
- 18.5 All high-risk breaches will be investigated formally by the Data Protection Officer and reported to the Finance & Resources Committee annually. Where an investigation identifies a case to be answered by one or more members of Staff, this will be addressed through the Staff Disciplinary Policy, if appropriate.
- 18.6 The Chair of the Finance & Resources Committee will be responsible for providing the Corporation Board with a report of any breaches or issues in relation to Data Protection through the minutes of the Finance & Resources Committee and their presentation at Corporation Board meetings

19. INTERNATIONAL TRANSFERS

- 19.1 The College may transfer personal data outside the United Kingdom to other countries on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards (e.g., by way of binding corporate rules or standard data protection clauses) or where we obtain

the relevant data subjects' explicit consent to such transfers. Staff must not export any Personal Data outside the UK without the approval of the Data Protection Officer.

- 19.2 We will inform data subjects of any envisaged international transfers in our privacy notices.

20. TRAINING

- 20.1 Employees need to be adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this Policy or responding to subject access requests under this Policy, will receive additional training to help them understand their duties and how to comply with them.
- 20.2 Support colleagues with primary responsibility for processing of personal and sensitive information receive training appropriate to their day to day duties and are required to maintain a level of operational understanding and awareness for the implementation of this Policy and associated procedures. They will receive refresher training every year.
- 20.4 All College employees receive a level of training appropriate to their role, with refresher training every 3 years. This will be recorded and monitored through central Workforce Development Records.
- 20.5 Students and other stakeholders will receive information and briefings appropriate to the personal data they provide, process or have access to, ensuring that all are aware of their rights and responsibilities with regard to Data Protection.

21. CONSEQUENCES OF FAILING TO COMPLY

- 21.1 The College takes compliance with this Policy very seriously. Failure to comply with the Policy:
- 21.1.1 Puts at risk the individuals whose personal data is being processed;
 - 21.1.2 Carries the risk of significant civil and criminal sanctions for the individual and the College;
 - 21.1.3 May, in some circumstances, amount to a criminal offence by the individual; and,
 - 21.1.4 Damages the reputation of the College in the eyes of the public and its business partners.
- 21.2 Due to the importance of this Policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the College's procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this Policy, they may have their contract terminated with immediate effect.
- 21.3 A student breaching the Data Protection Policy, associated procedures and Codes of Conduct may be subject to disciplinary action under the College's procedures for student behaviour and conduct.

22. IMPLEMENTATION OF THE POLICY

- 22.1 The College will ensure that the policy is implemented consistently across the College.

23. MONITORING AND EVALUATION OF THE POLICY

- 23.1 The Data Protection Officer will monitor implementation of this policy and will report any issues arising to the Corporation.

24. REVIEW OF POLICY

- 24.1 The above policy will be reviewed by the relevant parties annually, or as required.

25. ENVIRONMENTAL IMPACT ASSESSMENT

- 25.1 The College is fully committed to the sustainability agenda.
- 25.2 All policies take into consideration, at the time of writing and approval with the Senior Leadership Team, their impact on the agenda.
- 25.3 Policies may not be approved or be amended if they impact significantly on our commitment to improving our carbon footprint and our corporate social responsibility.

26. GENERAL DATA PROTECTION REGULATION (GDPR)

- 26.1 All policies which are approved by the Senior Leadership Team are in line with our GDPR suite of policies and procedures.

EMPLOYEE/PERSONNEL RECORDS

Personal Data Held In	Retention Period	Reasons for Retention Period
Medical Records: Medical Records Cards, Medical Examinations and Health Questionnaires	30 Years after employment ceases	Commercially Sensitive
Accident Reports	Indefinite	Commercially Sensitive
Details of Medical Schemes	Indefinite	Commercially Sensitive
Organisation Charts	Indefinite	Commercially Sensitive
Staff Personnel Records	7 Years after employment ceases	Statute of Limitations
Salary Registers	6 Years	Taxes Management Act
Expense Accounts/Records	7 Years	Statute of Limitations/Taxes Management Act
Overtime Records/Authorisation	3 Years	Commercial/audit
Claims for Redundancy and Long Service Award	7 Years after employment ceases	Statute of Limitations

PAYROLL DOCUMENTATION

Personal Data Held In	Retention Period	Reasons for Retention Period
Income Tax Records Re: Employees	6 Years	Taxes Management Act
Notice to Employer of Tax Code	6 Years	Taxes Management Act
Certificate Of Pay and Tax Deducted	6 Years	Taxes Management Act
Notice of Tax Code Change	6 Years	Taxes Management Act
Annual Return of Taxable Pay and Tax Deducted	6 Years	Taxes Management Act
Records of Pension Deductions (Including Superannuation)	6 Years	Pensions Act 1995
Clock Cards	2 Years	Audit
Copy Pay Slips	2 Years	Commercial and Audit

STUDENT RECORDS

Personal Data Held In	Retention Period	Reasons for Retention Period
Student Enrolment Forms (Paper)	2 Years	Electronic Data relied on once all data input
Student Records, Relating to Academic Achievement and Conduct	6 Years	Limitation Period for Litigation
Student Data - Alphabetical Listings	10 Years	ESFA Funding Requirements
ESFA Data Returns	10 Years	ESFA Funding Requirements
Student Registers	10 Years	ESFA Funding Requirements

STATUTORY RECORDS

Personal Data Held In	Retention Period	Reasons for Retention Period
Details Re: Current Pensioners	10 Years after benefit ceases	Commercial
Changes of Payment	6 Years	Statute of Limitations
Payroll Control Account	7 Years	Statute of Limitations and Taxes Management Act.
All Trust Deeds and Rules	Indefinite	Companies Act, Commercial and Pensions Act 1985
Trustee Minute Book	Indefinite	Companies Act, Commercial and Pensions Act 1985
Governor Records	2 Years after cessation	Members' Report and Financial Statements.
Annual Accounts	Indefinite	Companies Act, Commercial and Pensions Act 1985
Investment and Insurance Policy Records	Indefinite	Companies Act, Commercial and Pensions Act 1985
Actuarial Reports	Indefinite	Companies Act, Commercial and Pensions Act 1985
Contribution Records	Indefinite	Companies Act, Commercial and Pensions Act 1985
Group Health Policies	12 Years after final cessation of benefit	Statute of Limitations

PURCHASE INVOICES AND SUPPLIER DOCUMENTATION

Personal Data Held In	Retention Period	Reasons for Retention Period
Payment Cash Book or Record of Cheque Payments	6 Years	Companies Act/Charities Act
Purchase Ledger	6 Years	Companies Act/Charities Act
Invoice - Revenue	6 Years	Companies Act/Charities Act
Invoice - Capital Item	10 Years	Companies Act/Charities Act and Commercial Considerations
Invoice - Subcontractor Training: All Subcontractor Documents regarding Student Participation, both Manual and Electronic Documents, must be submitted to the College, at the Completion of the Contract, in order that they can be retained correctly.	See Note 1	ESF Policy Directive
Successful Quotations for Capital Expenditure	3 Years	Commercial and Audit considerations
Petty Cash Records	7 Years	Companies Act, Charities Act and VAT.

NOTE 1: Where any documents are required to support a claim for ESF funding, the retention period will be extended to three years after the European Commission has made the final payment for the programme. Prior to the destruction of any records; it is the responsibility of the Manager who “owns” the documents to confirm:

- (i) whether they are required to support an ESF Funding Claim and
- (ii) the actual retention date for that ESF Funding Programme.

Information regarding retention periods for ESF programmes can be obtained on-line.