European Union
European
Social Fund

Swindon College

It is intended that this policy is 'fair to all'. Where any part could potentially lead to unequal outcomes, the policy then justifies why this is a proportionate means of achieving a legitimate aim.

Institutional Policies, Procedures, Practices

Title:	**DATA PROTECTION POLICY**
Owner:	**CIS Manager**
Date:	**June 2018**
Review Date:	**June 2020**
Approval Reference:	**CLT/SLT**

____

1. Introduction

The 2018 Data Protection Act and General Data Protection Regulations (GDPR) regulates how organisations may use personal data and protects the rights of individuals with regard to the use of their personal data.

The Act re-enforces 6 principles that apply to the use of personal data.

The Data Protection Act principles are:

- The processing of personal data must be lawful, fair and transparent.
- The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and must not be processed in a manner that is incompatible with the purpose for which it is collected.
- Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Personal data undergoing processing must be accurate and, where necessary, kept up to date.
- Personal data must be kept for no longer than is necessary for the purpose for which it is processed.
- Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

The use of personal data is also governed by other statutory and common law requirements, including the laws of confidence and defamation. Swindon College is committed to ensuring that its use of personal data is fully compliant with the law and best practice and to this end has approved this Data Protection Policy.

2. Objectives

The purpose of this policy is to set out clearly Swindon College's Policy in respect of Data Protection and the procedures to be followed by College staff and students.

3. Scope

This policy applies to:

- all students
- permanent, fixed term and temporary staff
- Governors
- secondees
- third party representatives
- partners
- contractors and sub-contractors
- consultants
- agency workers
- volunteers
- interns
- apprentices
- agents
- sponsors engaged with the college

4. Personal & Sensitive Data

4.1 Personal Data

Personal data is information that relates to an identified or identifiable individual and could be as simple as a name, address or tel. no, or other identifiers such as a student or staff ID no, Unique Learner Number, name abbreviations, an IP address or a cookie identifier.

If it is possible to identify an individual directly from the information processed, then that information may be personal data.

If an individual cannot be identified directly from the information, then it should be considered whether the individual is still identifiable. College Staff and Students should take into account the information being processed together with all the means reasonably likely to be used by a person to identify that individual.

Information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

4.2 Special Category Data (Sensitive Data)

Special category data is more sensitive, and so needs more protection.

Special category data includes:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

5. Data Breaches

5.1 Definition of a Data Breach

An event which has caused or has the potential to cause damage to an individual's or Swindon College's information assets or reputation.

Examples are:

- Accidental loss or theft of personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use of personal data
- Access to or modification of data or information systems
- Accidental or deliberate sharing of user login details to gain unauthorised access to systems
- Accidental or deliberate unauthorised disclosure of personal data, sensitive or confidential information
- Email sent to an incorrect recipient
- Document posted to an incorrect address or addressee
- Accidental disclosure of user login details
- Equipment failure
- Malware infection
- Disruption to or denial of ICT services

5.2 Data Breach Reporting

When a member of staff or student suspects a data breach they, should immediately notify the College Data Protection Officer dataprotection@swindon.ac.uk with full details of the breach. If the member of staff or student has been the cause of the breach or part of a process that has led to the breach, the person should not continue with that process until investigation has completed.

The Data Protection Officer will:

- investigate the nature of the breach, the type of data involved, and where personal data is involved, who the subjects are and how many personal records are involved. The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident; for instance whether harm could come to individuals or whether data access or ICT services could become disrupted or unavailable.

- take appropriate action to prevent the breach from escalating.

- inform those individuals without undue delay if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.

- keep a record of the data breach regardless of whether the College is required to notify the ICO.

- Assess whether the ICO should be notified of the breach within 72 hours of becoming aware of the breach, where feasible.

If the investigation finds a possible breach then depending on the importance of the breach the DPO may seek advice from the ICO. The Data Protection Officer reserves the right to seek the advice from the ICO on any matter that is not trivial.

If the DPO is satisfied that the integrity of the College is still intact, the breach can be dealt with internally. A review of internal procedure and process may be needed, or a more detailed investigation may be carried out.

6. Responsibilities

This part of the Policy identifies the Data Protection responsibilities of various members of staff and students.

6.1 Senior Leadership Team and College Leadership Team

The Senior Leadership Team (SLT) and College Leadership Team (CLT) is committed to ensuring that the College is fully compliant with the law and best practice for handling personal information. To this end the SLT and CLT will:

- Approve College policies & procedures for handling personal data;
- Review developments in good practice and in particular, any Codes of Practice issued by the Information Commissioner having a bearing on College activities, updating College policies and procedures, as appropriate;
- Allocate resources (staff time and budget) to enable the Data Protection Action Plan to be delivered and compliance of the Data Protection legislation.
- Determine the College's Records Management and Information Strategies concerning how information, including personal data, is organised, categorised, stored and retrieved.
- Ensure all College staff and Students receive Data Protection training.
- Appoint a Data Protection Officer reportable to SLT.

6.2 Data Protection Officer

The Data Protection Officer will be responsible for maintaining the College's Data Protection system (its policies and procedures).

The Data Protection Officer will:

- Maintain the College's Data Protection Registration with the ICO;
- Monitor ICO guidance, data protection legislation and GDPR;
- Make recommendations to the Leadership Team on good practice and Data Protection policy;
- Provide training, guidance, disseminate information and advise on any specific Data Protection issues;
- Deal with Subject Access requests and co-ordinate responses to complaints that have a bearing on other data subjects rights (unwarranted substantial damage or distress; direct marketing; rectifying,

blocking, erasing & destroying inaccurate personal data and disputed cases of inaccuracy or other alleged breaches);

- Manage data breach process;
- Co-ordinate and advise on all non-routine requests for disclosure of personal information;
- Investigate personal data breaches in line with Data Protection legislation and General Data Protection regulations;
- Undertake periodic data protection audits and Privacy Impact Assessments;
- Review College policies and procedures in line with The Data Protection Action 2018 and GDPR;
- Maintain the College Data Asset Register.

6.3 Responsible Managers

Personal data is processed across the breadth of the College's normal everyday activities. Good personal data handling is one aspect of what employees need to do to deliver excellent services to students and internal customers. The key to achieving high standards in handling personal information is recognising that the primary responsibility for complying with legislation and good practice lies with those staff and managers who are responsible for deciding how in practice personal information will be used. The line managers of departments who process personal information are the responsible managers for this policy.

Responsible Managers will, in respect of their departments:

- Ensure that they are satisfied with the legality of holding the information and how it is used;
- Ensure that they have written documentation assessing & identifying legitimate grounds for processing personal data and sensitive personal data;
- Make appropriate provision for the security of both manual and computerised personal data where held locally (Back-up, contingency plans for catastrophic failure/migration of data to new systems, access to physical environment, locked files, guidelines on processing off-site, secure disposal etc). The security arrangements for computerised personal data must comply with the College's IT Policy;
- Ensure Staff only have access to data including network drives required for their role.
- Ensure that staff with access to personal data receive appropriate guidance and training covering:
    - The security arrangements for the data
    - How personal data is to be collected and recorded including approved sources
    - How consent is to be obtained where this is the ground for processing personal information
    - The information data subjects are entitled to receive under the Fair Processing Code and that application forms etc include this information
    - Any permitted routine disclosures of the data and how to respond to other requests for disclosure;
    - Procedures for regularly reviewing personal data to check that it is adequate, accurate, up to date, not excessive and deleted when no longer needed;

- Refer any non-routine requests for disclosure to the Data Protection Officer;

- Promptly inform the Data Protection Officer of any requests for subject access so that they can be responded to within the appropriate time limits.

- Be aware of data subjects rights to compensation in certain cases and their right to rectify, block, erase & destroy inaccurate personal data and inform the Data Protection Officer of any complaints alleging breaches of the Act or any cases where the data subject's complaint of inaccuracy is disputed;

- Ensure that personal data are not transferred outside the EEA other than in accordance with the Act;

- Ensure that any processing of personal data that is carried out by a contractor on behalf of the College is subject to a written contract that requires the data processor to act only on instructions and makes appropriate provision for the security of the data.

- Report any suspected data breach to the Data Protection Officer immediately.

- Retain and archive personal data in line with the Retention and archiving section of this policy.

6.4 Computer Services

All staff and users of personal data have some responsibility for the security of that data. IT services have an important role in ensuring the security of computerised data.

In particular they will:

- Be responsible for advising the College on the state of technological development with regard to IT security
- Back up data on the College's servers and IT systems

- Implement virus detection software and measures to prevent malicious software spyware, and hacking;

- Place restrictions on access so that individuals only have access to personal data in which they have a legitimate interest;

- Require the use of complex passwords and ensure that they are changed regularly;

- Promote and police policies for use of College systems and IT facilities including e-mail, intra and Internets that ensure compliance with the College's Data Protection obligations and investigate breaches of IT security and report suspected data breaches to the Data Protection Officer.

- Ensure all laptops have BitLocker installed.

6.5 Human Resources

An important aspect of security is ensuring the reliability of staff. The Human Resources team can contribute to this aim in a number of ways. They will:

- Ensure that the College's Employment Practices are consistent with the Information Commissioner's Employment Practices Code of Practice;

- Ensure that the Data Protection obligations of staff are reflected in the College's Disciplinary Procedures and contracts of employment;

- Ensure that all staff are aware of the types of personal information that the College will routinely make public (e.g. name, post, academic qualifications, College telephone and e-mail) and that individuals have the right to object to that disclosure where they consider it may cause them substantial damage or distress;

- Provide advice to responsible managers and others on the application of the pre-employment vetting process.

- Report any suspected personal data breach to the Data Protection Officer.

6.6 All Staff

All staff are likely to use and have access to some personal data in the course of their duties, for example other staff, students or members of the public.

They will:

- Respect the privacy and confidentiality rights of all data subjects. In particular they should be careful that personal data are not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party. (Unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases). This includes making sure that casual access to data is not possible, (for example by members of the general public seeing computer screens or printouts).

- Only use personal data for approved purposes and ensure that they comply with any instructions and guidelines they are given about the use of personal data

- Inform the 'Responsible Manager' of any proposed new uses of personal data

- Keep all personal data secure and not remove it from College premises without the permission of the appropriate 'Responsible Manager'

- Comply with all College policies regarding the use of IT facilities, e-mail and Inter/Intranets

- Check that the information they provide to the College in connection with their employment is accurate and up to date and inform the College of changes to or errors in information held.

- Report any suspected personal data breach to the Data Protection Officer.

- Ensure the email and SC Connect messaging etiquette is followed during all communication.

- Contact the Data Protection Officer with any data protection queries.

6.7 Students

Students will not normally process personal data in the course of their studies or in other ways on behalf of the College. However, where from time to time this happens, they will need to inform their tutor and comply with the Guidelines and any other instructions given to them.

At all times students will:

- Respect the privacy and confidentiality rights of all data subjects
- Not seek to use or gain unauthorised access to personal information
- Comply with all College policies regarding the use of IT facilities, e-mail and Inter/Intranets
- Check that the information they provide to the College in connection with their studies is accurate and up to date and inform the College of changes to or errors in information held
- Report any suspected personal data breach to the Data Protection Officer.
- Contact the Data Protection Officer with any data protection queries.
- Ensure the email and SC Connect messaging etiquette is followed during all communication.

7. Misuse of Data

Disciplinary action, including dismissal, may be taken against any employee who contravenes any instruction contained in, or following from, this Data Protection Policy and Guidelines issued by Swindon College. Upon discovering that this Policy is not being complied with, or if an intentional breach of the Data Protection Principles has taken place, the Data Protection Officer in consultation with the senior team, shall have full authority to take such immediate steps as considered necessary.

8. Data Retention and Archiving

8.1 Data Retention Periods

ALS – Bank staff contact information	Duration of contract
ALS – Learner Difficulty on EBS	1 year (deleted every December the following academic year)
ALS – SSW timetable including student names	Current Academic year
ALS – Staff signing in register	1 term
ALS – Tracking Register	1 year
Annual Leave records (overtime and time in lieu)	1 year (after leave period)
Application Forms	Current Year
Assessment – Conflict of Interest register	3 years
Assessment and Verification records	3 years
CCTV images	30 days
Class Registers / Contact sheets	31th December 2030
Coaching Logs – staff	6 years
Copies of Examination Records	31th December 2030
Course Files – O:Drive	3 years
Enrolment Forms	31th December 2030
Estates – Call out rota	Current Academic year
Estates – Call out rota telephone numbers	Duration of contract
Estates – Contractor contact information and insurance	Duration of contract
Estates – Eye care voucher – names of staff	2 years
Estates - Mini bus usage - names of staff and driving license and MIDAS test date	1 year
Estates – VAT numbers	Duration of contract
Examination results (copies)	31th December 2030
Finance Documents	7 years
Finance Documents (certain Finance documents for auditing and accounting purposes)	3 years
General Correspondence	2 years
HE – Academic misconduct minutes	Duration of course
HE – Complaints and Grievances	Duration of course + 1 year
HE – Council Tax forms	Duration of course
HE – Disability Records	Duration of course +1yr (CIS 7yrs)
HE – Exam board minutes	5 years
HE – Hardship Forms	Duration of course + 1 year
HE – Job descriptions	Indefinitely – regular updates
HE – Letters to students	Duration of course + 1 year
HE - Mitigation circumstances information, medical records, police records, any evidence for a Mitigating Circumstance Claim	Duration of course

HE – Programme Committee minutes	Duration of course + 1 year
HE – Student Feedback	Duration of course + 3 years
HE – Students marks and results	7 years
HE – Student work for external examiners	Duration of course
HE – University Contacts	1 year
Health and Safety Information – Contact H&S Manager for further information regarding specific requirements	3 - 50 years
Human Resource files - Current and Former Employees	6 years from leave date
Management Accounts	Current Academic year
Marketing – Case Study Information	1 year
Marketing – Images and videos of learners	2 years
Marketing – Learner names and contact information	1 year
Marketing – Student Photos for Prospectus	1 year
Meeting minutes	3 years
Nursery Records – children's information, safeguarding and medical information	24 years in line with National Day Nursery Association (NDNA)
Nursery – all other information	5 year from date of closure
Observation Records	6 years
Part time teaching contracts	6 years
Payroll Information	Unlimited
Pension record	Unlimited
Photography / Video for marketing purposes	2 years
Photography / Video for courses related assessment purposes	3 years
PRADAS held by HR	6 years
PRADAS held by manager	1 academic year
Programme Area file – copies of internal transfers	2 years
Programme Area file – copies of return of absences, overtime/PT teaching claims	2 years
Progress Monitoring minutes	3 years
Property Matters	12 years
Property matters - where they relate to title for existing assets, records	unlimited
Quiet Room Register	1 year
Safeguarding Files	unlimited
Sickness Records	6 years
Staff Photo for ID	For the duration of the employment
Student Access Arrangements	Academic Year
Student Photos for ID	For the duration of the course
Student Records for CIS, Business First and Exams	31st December 2030
Student work / coursework (competency based)	Until External Moderation visit
Student work / coursework (non-competency based)	3 months
Training Logs for awarding organisations and OFSTED	Completion of programme +5 yrs
Trips - Copies of passports EHIC cards visas etc	Duration of trip
Unsuccessful Staff Applicants records	2 years from closure of campaign

8.2 Archiving

Records for archiving should be filed in archive storage box with details of the owner and destroy date in line with the retention period listed above.

The Head of Department is responsible for maintaining a record of the data retained within the archive in line with the College data retention periods.

The Estates department are responsible for:

- ensuring the archived records are retained in a secure, water and fireproof environment.
- retrieving the archived records within 2 days of receipt of a request for the records
- destroy the records retained within the archive on the destroy date on the box.

9. Privacy Notices

Details of staff and student privacy statements are available on the College the website

https://www.swindon.ac.uk/Privacy-Policy.aspx

These set out how personal information is used and in particular:

- Why the College collects personal information
- The personal information that the college collects
- How the College collects the personal information
- How the personal information is stored
- How the College uses the personal information
- The legal basis on which the College collects and use personal information
- Who has access to personal information
- How the College shares personal information
- The transfer of personal information outside of Europe
- How the College protects personal information
- How long the College retains personal information
- An individual's rights over personal information

10. Subject Access

10.1 General Enquiries

A student or member of staff can ask the College to see information that the College holds about them by making a general enquiry to the appropriate department, such as how much they owe the College in fees if they are a student. The College may carry out identity checks to ensure that they are who they say they are, but in general, the information will be disclosed to them.

10.2 Data Subject Access Requests

An individual also has a legal right under the Data Protection Act 2018 and GDPR to be informed about whether or not any information is held about them and to see a copy of it. This is known as a right of Subject Access. Swindon College Students and Staff have the right to:-

- A copy or description of the information that the College holds about them. This information may be held electronically (for example on computer, closed circuit TV, video or audio recordings) or in paper records. The College will provide the information in an electronic format where possible. Paper records will be scanned unless the original paper copy is requested.
- The personal data will be provided in a structured, commonly used and machine readable format unless the original paperwork is requested. Formats will include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data if required.
- The College will explain any technical terms or abbreviations so that they can understand what they mean.
- Be informed about the purpose(s) for which the information is processed.
- Be informed about the source(s) of information and recipient(s) or classes of recipients to whom the College may have disclosed the information.

Students have the right to see some exam-related information, such as marks, examiner's comments and minutes of examination appeals panels. If a student asks for exam results before they have been announced, the College will respond within 30 days from when the individual’s results are published.

There may be circumstances where not all information about an individual can be provided. There may be exemptions under the Act that the College needs to apply, these are:

- Crime prevention and tax collection
- Immigration control
- Required by law / legal proceedings
- Regulatory functions
- Third party data
- Management forecasts / negotiations
- Confidential references
- Exams, scripts and marks
- Health, social work, child abuse and education records (serious harm)

10.3 Timescale

The College will endeavour to reply promptly to the request within one month, provided that the college has evidence of the individual’s identity and enough information to search for the information. Where the college asks for additional information, the one month countdown starts when the additional information has been received.

This can be extended by two months where the request is complex or a number of requests have been received. The College will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where the College is not taking action in response to a request, the College will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

10.4 Cost

There will be no cost for a subject access request unless the request is manifestly unfounded or excessive by the data subject such as a repeated request.

Where a request from a data subject is manifestly unfounded or excessive, the College may charge a reasonable fee for dealing with the request or refuse to act on the request.

The fee will be determined the cost to the College.

10.5 How to Make a Subject Access Request

Data Subject Access should be emailed or sent in writing to the College Data Protection Officer – dataprotection@swindon.ac.uk

The individual will need to provide:

- The necessary information from the individual to confirm the individual identity. Please provide a photocopy of any of the following items:-
    - Birth certificate, marriage or civil partnership certificate, driving licence (photo card or paper), passport, two different utility bills (for example gas, electricity or water).
- Sufficient information from the individual to help the College locate the information that the individual have requested.

The College Student or Staff member should provide as much information as they can to help the College locate the information, for example how far back in time the individual would like the College to search, or providing names of members of staff who the individual has been in contact with or specific areas in the College where the individual thinks that information may be held.

The information that the individual provides will be used to manage and administer the individual's request and carry out searches for information that is held about the individual.

10.6 Requests on Behalf of Other People

An individual may make an access request on behalf of another person. The College will send them a copy of information held only with the consent and authorisation of the subject.

If a parent or guardian makes a request on behalf of an individual person under 18, the College may make additional enquiries to confirm that they have parental responsibility before releasing information. This may involve discussing the request with staff members within the College or with relevant external organisations.

10.7 Information That Relates to Other People

Under the Data Protection Act 2018, an individual is only entitled to see information that is held about them. There may be occasions when information about other people is held on the individuals' records. The College may inform the third party that a subject access request has been made and inform them that their personal data is contained within the request. The College may contact the third party for their consent to release information that identifies or relates to them. The College is entitled to withhold information about the subject if the third party consent has been withheld or cannot be obtained.

10.8 Automated Decision Taking

The College does not make decisions solely based on automated decision-making.

10.9 Correction or Deletion of Inaccurate Information

On receipt of a correction or deletion of inaccurate information the College will investigate the inaccuracy and any changes will be made within one month.

This can be extended by two months where the request is complex or a number of requests have been received. The College will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the individual have any queries, or need assistance with making a request, please contact the College Data Protection Officer: dataprotection@swindon.ac.uk

10.10 Further information

Impartial information and advice is available from the Information Commissioner's Office. The website is available at www.ico.org.uk.

11. College Forms and Procedures

All college forms and procedures must be reviewed by the College Data Protection Officer who will assess for Data Protection Act 2018 and GDPR requirements.

11.1 Forms

All college forms must include:

- Why the college is collecting the data
- How long it is retained and that it is destroyed
- Where it is stored (electronically and paper based)
- Who has access to it
- Who it is shared with

11.2 College procedures

College Procedures and amendments must be approved by the Data Protection Officer as part of SLT approval.

12. Glossary of Terms

Data

Data is information, which is processed automatically (by a computer), or is manual data which forms part of a relevant filing system. A relevant filing system is a system that is structured either by reference to an individual or by criteria relating to individuals so that specific details relating to a particular individual may be easily selected from that system. Data can be written information, photographs, or information such as fingerprints or voice recordings.

The Freedom of Information Act extends the definition of data to include unstructured manual data that is held for personnel purposes - where employees request to have access to their own personal data.

Personal Data

Is information that relates to a living individual who can be identified from that data and other information in or likely to come into the possession of the Data Controller (the College)? The Act **does not apply** to statistical or anonymised information where individuals cannot be identified, neither does it apply to people who are deceased.

Processing

Is anything done with the data including holding and viewing data. It includes

- obtaining
- holding
- amending
- collating and compiling
- reading and consulting
- disclosing
- transferring
- blocking, deleting or destroying information

If the individual have personal data in the individual's possession, the individual should assume that the individual are processing it.

Data Subject

The Data Subject is the individual who is the subject of personal data. This will include staff, students, suppliers of goods and services etc.

Data Controller

The Data Controller is the legal person or body who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. The College is the Data Controller.

Data Processor

Is any person other than an employee of the Data Controller who processes data on behalf of the Data Controller.

Third Party

Is any person other than the Data Subject, the Data Controller, the Data Processor or other person authorised to process data for the Data Controller.