DATA PROTECTION POLICY

January 2024

Key Details

Policy Title:	Data Protection Policy
Created By:	Data Protection Co-Ordinator
Approved By:	Data Protection Officer
Date of Approval:	22 January 2024
Review Date:	January 2026
Responsible Manager:	Director, MIS
Policy Category:	Data Protection
Related Policies:	Data Protection Retention Schedule
Policy Location:	Sharepoint Policy Hub

1. Introduction

The Data Protection Act 2018 and UK General Data Protection Regulation (UK 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 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. New College Swindon 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 New College Swindon's Policy in respect of Data Protection and the procedures to be followed by College staff and students.

This Policy (and the other policies and documents referred to in it) 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.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

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 telephone number, or other identifiers such as a student or staff ID number, 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 the individual cannot be identified by one piece of data alone, however with additional knowledge the individual can be identified, this is still personal data.

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

Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Reporting process. Please familiarise yourself with it

as there are important obligations which College Staff need to comply with in the event of Personal Data breaches.

A Personal Data Breach is an event which has caused or has the potential to cause damage to an individual's or New College Swindon's information assets or reputation.

A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. 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:

1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data eg, hacking, accessing internal systems that a College Personnel is 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 student, or disclosing information over the phone to the wrong person;

2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data eg, loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

3. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

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@newcollege.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 (DPO) 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 Information Commissioner's Office (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 DPO 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. All breaches will be reported to Senior Leadership Team (SLT), College Leadership Group (CLG) and the Governing Body.

A failure to report a breach when required to do so could result in a fine as well as a fine for the breach itself. Fines may be imposed by the ICO amounting to 10 million euros or 2 per cent of global turnover.

6. Responsibilities

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

6.1 Principalship and Senior Leadership Team

The Principalship and SLT is committed to ensuring that the College is fully compliant with the law and best practice for handling personal information. To this end Principalship and SLT 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 (DPO)

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

The DPO will:

- Maintain the College's Data Protection Registration with the ICO;
- Monitor ICO guidance, data protection legislation and GDPR;
- Make recommendations to the Senior 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);

- Co-ordinate and advise on all non-routine requests for disclosure of personal information;

- Manage data breach processes and Investigate personal data breaches in line with Data Protection legislation and General Data Protection regulations;

- Undertake periodic data protection audits and Data Protection Impact Assessments;

- Review College policies and procedures in line with The Data Protection Action 2018 and GDPR;

- Maintain the College Record of Processing Activities (RoPA).

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 DPO 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 DPO 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 DPO immediately.

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

- Undertake a Data Protection Impact Assessment (DPIA) for the introduction of any potential high-risk situation for example where new technology is being deployed or where a profiling operation is likely to significantly affect individuals. If the DPIA indicates high risk processing this will be discussed with the Senior Leadership Team which may result in the ICO being consulted.

- Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

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:

- Undertake a Data Protection Impact Assessment (DPIA) for the introduction of any potential high-risk situation for example where new technology is being deployed or where a profiling operation is likely to significantly affect individuals. If the DPIA indicates high risk processing this will be discussed with the Senior Leadership Team which may result in the ICO being consulted.

- Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

- 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 to identify potential data breaches;

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

- Passwords must be changed in accordance with IT Policy

- 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 DPO.

- 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 (eg, 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 DPO.

6.6 Marketing

The Head of Marketing will ensure that consent is obtained for the purpose of marketing courses and events at New College Swindon and photography and video usage.

6.7 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
- Ensure USB memory sticks (for Awarding Body purposes only) and personal devices are encrypted and/or password protected.
- 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. Refer to section 4 for what is personal data.
- Contact the Data Protection Officer with any data protection queries.
- Ensure no third party is engaged to process data without written authorisation from the Senior Leadership Team.
- Not access College systems outside of the EEA (European Economic Area)
- All teaching staff are responsible for access to their online live streaming sessions and recordings.

6.8 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 DPO.

- Contact the DPO with any data protection queries.

7. Appointing Contractors who Access the College's Personal Data

If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

Any contract where an organisation appoints a Processor must be in writing.

You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it, they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

GDPR requires the contract with a Processor to contain 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 GDPR or other EU or member state data protection law.

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.

8. 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 New College Swindon. 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 SLT, shall have full authority to take such immediate steps as considered necessary.

9. Retention, Archiving and Destruction

9.1 Archiving and Destruction: Personal Data must not be kept for longer than needed

Data Protection Laws require the College does not keep personal data longer than is necessary for the purpose or purposes for which the College collected it.

Data retention periods for personal data we process are detailed within the College Data Protection Retention Schedule. Further information can be provided on request to the Data Protection Co-ordinator via the DataProtection@newcollege.ac.uk email.

If College staff feel that a particular item of personal data needs to be kept for more or less time than the retention period, for example, because there is a requirement in law or, if College staff have any questions about this policy or the College's retention practices, they should contact the Data Protection Officer.

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 Senior Manager for a department is responsible for maintaining a record of the data retained within the archive in line with the College data retention periods.

The Estates/Facilities department is 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
- confidentially destroying the records retained within the archive on the destroy date on the box.

10. Data Quality: Ensuring the use of accurate, up to date and relevant personal data

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 (see paragraph 9) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

All College Staff 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.

All College Staff that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and 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 College Staff to independently check the Personal Data obtained.

In order to maintain the quality of Personal Data, all College Staff 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 (eg, for legal reasons or that which is relevant to an investigation).

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. The College has a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

11. Transparent Processing: Privacy Notices

Details of student and staff privacy notices are available via our websites and staff portals.

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

12. Subject Access: Individuals' Rights

GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR.

The different types of rights are reflected in this paragraph.

12.1 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.

12.2 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. New College Swindon 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)

12.3 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.

12.4 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 by the cost to the College.

12.5 How to Make a Subject Access Request

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

The individual will need to provide:

- The necessary information from the individual to confirm the individual identity. Please provide 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 has 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.

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

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.

12.7 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.

12.8 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; and
- the Personal Data has to be erased for compliance with a legal obligation.

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.

12.9 Right of Data Portability

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.

12.10 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 has any queries, or need assistance with making a request, please contact the College Data Protection Officer: DataProtection@newcollege.ac.uk

12.11 Further information

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

13. Marketing and Consent

The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing activities, it will do so in a legally compliant manner.

Marketing consists of any advertising or marketing communication that is directed to particular individuals.

Privacy and Electronic Communications Regulations (PECR) sit alongside data protection and apply to direct marketing ie, a communication directed to particular individuals and covers any advertising/marketing

material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

Consent is central to electronic marketing and the College uses opt-in boxes as a default.

The College uses a "soft opt in" if the following conditions are met:

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- the College are marketing its own similar services; and
- the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

14. Automated Decision Making and Profiling

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

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 College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

The College does not carry out Automated Decision Making or Profiling in relation to its employees.

15. Data Protection Impact Assessments (DPIA)

The GDPR introduced a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The College uses a standard template using the ICO's standard DPIA as a template.

The College's standard format DPIA is available on the College website and from the Data Protection Co-ordinator.

Where a DPIA reveals risks, which are not appropriately mitigated the ICO must be consulted by the DPO.

Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

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):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences eg, the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale eg, CCTV cameras.

All DPIAs must be reviewed and approved by the Data Protection Officer.

16. Transferring Personal Data to a Country outside the 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. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

So that the College can ensure it is compliant with Data Protection Laws College, Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

17. College Forms

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.

17.1 Forms

All college forms must include:

- The information that you give us;
- the uses made of your personal information;
- the legal basis on which we collect and use your personal information;
- how long we keep your personal information;

- how we share your personal information;
- how we transfer your personal information outside Europe;
- will we monitor your use of the College's IT; and
- your rights over your personal information.

18. Glossary of Terms

College – New College Swindon; Queen's Drive Campus, New College Drive, Swindon, SN3 1AH; North Star Campus, North Star Avenue, SN2 1DY

College Personnel – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

Controller – Any entity (eg, 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. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

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.

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.

Data Protection Officer – The College Data Protection Officer is the Director of MIS at New College Swindon.

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.

EEA – 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.

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Individuals – 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 partnerships and sole traders.

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, 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

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 has personal data in the individual's possession, the individual should assume that the individual is processing it.

Processor – Any entity (eg, 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 a 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. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

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 (ie, information about their inherited or acquired genetic characteristics), biometric data (ie, information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

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.

If you require any further information or have any questions or queries relating to this document, please contact the Data Protection Officer: DataProtection@newcollege.ac.uk.