GENERAL DATA PROTECTION REGULATION POLICY

Table of Contents

POLICY FOR ALL STAFF AND STUDENTS

1.0 Introduction

1.1 The General Data Protection Regulation (GDPR)

The Data Protection Act 1998 has now been superseded by the Data Protection Act 2018. This new act brings in new data regulations commonly known as General Data Protection Regulation (GDPR). The new regulations significantly extends the scope of data protection law. It applies to all personnel data held not just those in electronic form. As a result of the Colleges Incorporation on 1 April 1993, the College became wholly responsible for compliance with GDPR.

The College needs to record:-

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purpose and lawful reason for the processing the data
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

The GDPR also lists individual's rights on the data being held and that college must do Data Impact assessments when using new technologies or that processing is likely to result in a high risk to the rights and freedoms of individuals e.g. large scale, systematic monitoring of public areas (CCTV).

2.0 Obligations under the GDPR

2.1 The College must appoint a Data Protection Officer

The College as a body corporate is the data controller in GDPR, and the Board is therefore ultimately responsible for implementation. However, the designated data protection officer will deal with day-to-day matters.

The designated data protection officer for Selby College is Mike Pilling [Network Services Manager].

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).
- The DPO reports to the highest management level of your organisation – ie board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.

- Adequate resources are provided to enable DPOs to meet their GDPR obligations.
- The professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interest conflicting positions within the organisation

2.2 Lawful processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing" under the DPA. It is important that you determine your lawful basis for processing personal data and document this.

- Lawfulness of processing conditions
- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

2.3 Individuals Rights

The GDPR provides the following rights for individuals:-

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

2.3.1 Right to be informed

The information you supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- Free of charge

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

2.3.2 Right of Access

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

Information must be provided without delay and at the latest within one month of receipt instead of 40 days under DPA 1998. People can make requests via a Data Subject Access request, a form for that purpose is at the end of this policy document.

Where requests are complex or numerous this period can be extend by a further two months. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

You must verify the identity of the person making the request, using "reasonable means".

You can't make request on other people's data only your own.

2.3.3 Right to Rectification and Erasure

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

The College can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

All staff, students and other users are entitled to know:

- What information the College holds and processes about them and why
- How to gain access to it
- How to keep it up to date
- What the College is doing to comply with its obligations under the GDPR 2018 Act.

The College must be prepared to answer the following kind of queries:

- Do you hold data about me?
- Please supply copies of all data you hold about me
- For what purpose do you hold data about me?
- To whom do you disclose data about me?

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on a computer or in any 'relevant filing system'. Any person who wishes to exercise this right should complete the college "Data Subject Access Request" form [See Appendix A] and give it to Data Protection Officer.

There is no charge for a subject access request, however, the college can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 1 month. Unless there is good reason for delay in such cases the time period can be extend by a further 2 months. The reason for delay will be explained in writing to the data subject making the request within the first month.

2.3.4 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

If the individual requests it, the college may be required to transmit the data directly to another organisation if this is technically feasible. However, the college is not required to adopt or maintain processing systems that are technically compatible with other organisations.

2.3.5 Right to object

Individuals have the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics.

If the personnel data is being processed for the purpose of direct marketing then:-

- The college must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- An objection to processing for direct marketing must be dealt at any time and free of charge.
- The college must inform individuals of their right to object "at the point of first communication" and in the college privacy notice.

3.0 GDPR Compliance

3.1 Data Audit

The College needs to be able to answer the following questions about the data it holds and processes

- What data do you hold and why?
- How do you collect the data?
- How and where is the data stored
- What do you do with the data?
- Who owns and controls the personal data?
- Retention and deletion
- Who is responsible for the data and processors associated with data?
- Do you have adequate technology / process to adequately manage data processing?
- Lawful basis for processing the personal data Article 6 and Article 9 where relevant.
- Is the data shared with any 3rd party

Therefore the college will maintain a Data Audit database containing the above information about all personnel data that is held in college. This will included data for example from MIS about students, HR about staff, CCTV, Finance and even data from Reception sign in book or the Salon customer list.

3.2 Lawful Processing of Data

The College needs to record the lawful reason for processing personal data. There are 2 Articles in the GDPR that control the processing of data. Article 6 reason and Article 9 reason (if required) will be recorded in the Data Audit database.

3.2.1 Article 6

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.2.2 Article 9

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

Special types of data include

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

There are ten conditions for processing special category data

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.3 Data Privacy Impact Assessments (DPIA)

The College must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals. E.g. large scale, systematic monitoring of public areas (CCTV)

3.4 Privacy Notices

The College needs to maintain privacy statements telling data subjects how the College is going to be using their personal data and their rights under GDPR. For convenience these notices will be published on the main college website (www.selby.ac.uk/privacy) and this web link can then be referred to in any documentation when gathering data e.g. Application/Enrolment forms and Job applications

In the first instance the college will produce 2 privacy notices, one for students the other for all other data subjects e.g. Staff & Governors.

The privacy notices need to cover the following items

- Who is collecting the data?
- Identity and contact details of the data controller i.e. Selby College
- Who is the Data Protection Officer (DPO)
- Which categories of personal data will you be collecting
  - Personal data
  - Personal sensitive
- Purpose of the processing and the legal basis for processing
- Why is it being collected?
- How else will the data collected be used?
- How is it collected?
- Identify the legal basis for processing either: consent, contract, legal obligation, vital interests, and legitimate interests.
- How will it be stored, securely?
- Who will it be shared with?
- Including any third parties the information is shared with
- Details of transfers to third country and the safeguards put in place to protect the individual's data.
- How long will you keep the data, giving reasons why that length of time in necessary and how that length of time was determined.
- Identify the existence of all the Users Rights and how users can access their rights:
  - the right to be informed;
  - the right of access
  - the right to rectification;
  - the right to erasure
  - the right to restrict processing;
  - the right to data portability;
  - the right to object; and
  - the right not to be subject to automated decision-making including profiling

The privacy notices need to be reviewed by the DPO if there any changes to how the college is handling data or every 3 years.

3.5 Third party processing and access to information

Sharing of data with a 3rd party is to be strictly controlled and should be done only for legal reasons (e.g. Police) or operational requirements (e.g. Exam boards, Government, franchise partners).

In addition to the data audit database a data sharing register needs to be maintained listing the data we share with 3rd parties. It will need to contain the following information about the 3rd party

- Data Processor Name e.g. OCR exam board
- Contact Details
- Scope & Description of Data being processed
- Lawful basis for sharing data
- Method of sharing e.g. secure web upload
- GDPR compliance statement from 3rd party

The Data Audit and Share Register databases once created needs to be reviewed at least annually by the Data Protection Officer and those that manage data in the college.

If we use a third party data controller to process data on behalf of the College we must ensure that the controller complies with the GDPR act. This would apply to subsidiary trading companies and franchise partners. We must obtain sufficient guarantees in respect of the processor's security measures and take reasonable steps to ensure compliance with those measures. We must ensure that the third party 'processor' is subject to a written contract with the College.

3.6 Transfer of information outside the United Kingdom and European Union

The College will not transfer data outside of the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

3.7 Retention of Data

Under GDPR the college needs to have a policy for how long it keeps personnel data.
This retention information should be in the Privacy Policies so staff and students are able to find and understand what is being done with their personnel data.

A more detailed log of retention times and why is to be recorded in the Data Audit database and how the data should be disposed of.

The principals are that:

- Information should only be stored for as long as is necessary
- Data must be securely destroyed once it reaches the end of its life

Each data set may have different retention lengths from 12 months to 10+ years and are largely governed by external obligations e.g.

- Legal requirements
- Financial Regulations
- Pensions requirements
- Funding requirements (e.g. record that student attended college and what they studied)

Some parts of the data sets may also need be deleted before the final record is disposed of e.g. Emergency Contact information for a student doesn't not need to be held for same length of time as the record that they attended the college.

3.8 Data Subject Consent

The GDPR sets a high standard for consent. In GDPR consent means offering individuals real choice and control. Genuine consent should put individuals in charge. Consents need to be refreshed if they don't meet the GDPR standard.

3.8.1 Asking for consent

Checklist for obtaining consent for personal data.

- Checked that consent is the most appropriate lawful basis for processing.
- The request for consent prominent and separate from other terms and conditions.
- Positively opt in.
- Don't use pre-ticked boxes or any other type of default consent.
- Clear, plain language that is easy to understand.
- Specify why we want the data and what we're going to do with it.
- Separate distinct ('granular') options to consent separately to different purposes and types of processing.
- Selby College and any third party controllers who will be relying on the consent are named.
- Tell individuals they can withdraw their consent.
- Ensure that individuals can refuse to consent without detriment.
- Avoid making consent a precondition of a service.

3.8.2 Recording and Managing Consent

- The college needs to keep a record of when and how we got consent from the individual.
- Keep a record of exactly what the individual was told at the time.
- Make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- Systems and processes must be able to record and act upon the withdrawal of consent at any time.
- Act on withdrawals of consent as soon as we can
- The college must also acknowledge the withdrawal of consent of the individual.

3.9 References

When a reference request is received, there is no legal obligation for one to be provided. The employee's explicit consent with be required to process the personal data which is contained within a reference.

3.9 Notification

Under GDPR the college no longer needs to notify the ICO in the same way as it did under the Data Protection Act 1998. However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

These fees will be used to fund the ICO's data protection work.

Currently the college is classified in Tier 1 for fees and will need to pay an annual fee of £55

3.10 Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may decide to withhold certificates, accreditation or references in the event that full course fees have not been paid, or all books and equipment returned to the college.

4.0 Data Breach

The following guidelines are to assist in dealing with a possible Data Breach in the college. This could be a loss of device, hacking, encryption, transmitting of personal information to the wrong party e.g. email

4.1 Investigate the Incident

Is the Incident a Personal Data Breach?

A personal data breach may involve loss of personal data or the unlawful accessing or processing of personal data. Only if an incident actually resulted in a breach of personal data the mandatory notification obligation applies. For instance, lost USB sticks, stolen laptops, malware infections or hacked databases containing personal data are considered personal data breaches.

A shortcoming in security measures, such as weak passwords or outdated software, are not considered a personal data breach as long as no personal data has been leaked.

4.2 Investigate the Scope, Nature and Possible Consequences

What is the source of the personal data breach?

Is it a stolen/lost device or hacking of service or inadvertent transmission of data to the wrong party?

How many individuals are affected by the personal data breach and is the data breach likely to result in a risk to the rights and freedoms of the individuals affected?

For example a hack of the MIS database could most likely have a severe impact on private lives of many people. On the other hand, a breach concerning only business contact details of one customer in SCBS may have minimal impact only.

Does the personal data compromised include sensitive data?

For example financial information, health data (from HR Info). Refer to data Audit spreadsheet for who controls the data for type of information that is held.

Was the compromised personal data encrypted or secured in a manner which makes it impossible for a third party to assess?

For example if adequate encryption is used or the data is adequately hashed and salted it can be assumed that third parties will not be able to access the personal data.
e.g. data stored on an laptop that has an encrypted hard drive

What steps are taken to mitigate (further) loss of personal data?

For example, disable accounts, change passwords, wipe all email data on smartphone. So that loss of personal data can be prevented or if access to hacked database could be regained, it is possible to mitigate further loss.

Which parties are involved in the data breach?

For example is it data on a 3rd party site e.g. BKSB data, Etracker or Onefile.

4.3 Investigate Notification Obligation to Supervise Authority

The ICO should be notified by the controller of any personal data breach that results in or is likely to result in ''a risk to the rights and freedoms of natural persons.'' This has to be assessed on a case by case basis.

For example, you will need to notify the ICO about a loss of student or staff details where the breach leaves individuals open to identity theft.
But the loss or inappropriate alteration of an internal telephone list would not normally meet this threshold.

It is relevant to know the answers to the above questions and have an idea of the reasonable consequences the breach may have (for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage).

If not yet all information is available, the controller should still notify the ICO.
If needed, the notification may be amended at a later stage when the full details are known or the notification could be withdrawn if not needed after all.
If notification to the ICO is required

Where a notification with the ICO is required please go to the following link for the latest guidance and procedure for reporting.

https://ico.org.uk/for-organisations/report-a-breach/
You can also call 0303 123 1113
If there is an Unlawful use of personal data breach (section 55), there is a PDF form to complete:-
https://ico.org.uk/media/for-organisations/documents/1432171/report-a-s55-incident.pdf

Details required will be

- The scope and nature of the personal data breach, including the categories and number of data subjects and data records concerned;
- The name and contact details of the data protection officer
- A description of the likely consequences of the personal data breach;

- A description of the measures taken or proposed to be taken to address the breach, including measures to mitigate any possible adverse effects.

4.4 Investigate Notification Obligation Individuals

Where a personal data breach is likely to result in a ''high risk'' to the rights and freedoms of individuals, you must notify those concerned directly. A ''high risk'' means the threshold for notifying individuals is higher than for notifying the ICO.

If affected individuals must be informed, you should provide at least the following information in clear and plain language:

- the scope and nature of the personal data breach;
- the name and contact details of the data protection officer
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to taken to address the breach including measures to mitigate any possible adverse effects (e.g. contact your credit card provider, change your password, etc.)

Notification to individuals shall not be necessary if the controller can demonstrate that ''appropriate technological protection measures'' were applied to the data concerned by the personal data breach, which ''shall render the data unintelligible to any person who is not authorised to access it.', such as encryption, or if it has subsequently taken measures which ensure that the high risk for the rights and freedoms of data subjects is longer likely to materialise.

If individual notifications would be a disproportionate effort, the controller can use some form of public communication instead provided that this will be equally effective in informing individuals.

The ICO have the power to overrule controllers and order them to notify the affected individuals if they disagree with a controller's assessment of the risk.

4.5 Create and Maintain an Internal Breach Register

The college is obliged to document any personal data breaches, which shall at least include information on the facts relating to the personal data breach, the effects of the breach and the efforts and remedial actions taken.

Also the college shall document any communication with ICO and affected individuals.
Plus in the event a decision was made not to notify supervisory authorities and/or affected individuals the facts and the reasons why such decision was made as the ICO may initiate an audit or request for information at any time.

4.6 Evaluate the Personal Data Breach and Update Technology and Policies

With GDPR there is new principle of accountability and it requires controllers to be responsible for and to be able to ''demonstrate'' and ''evidence'' compliance with the data protection principles, which include security obligations.

The Data Protection Officer needs to document what the college has done to prevent future personal data breaches originating from the same source as well as regularly reviewing and updating your breach detection, investigation and internal reporting procedures.

5.0 Responsibilities

The purpose of this section is to make all staff and students aware of their responsibilities towards all personal data held by the college and to indicate the practical steps to be taken to comply with the act.

5.1 The Data Protection Officer (DPO)

Is responsible for

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Selby College holds about them i.e. Subject Access Requests
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

5.2 The Network Services Manager

Is responsible for

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

5.3 Staff Responsibilities

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College. Any failures to follow the policy can therefore result in disciplinary proceedings.

Regarding the processing of personal data by the college, staff should ensure that any data, which it is proposed to process, are covered by the College's notification under the GDPR 2018. The processing of personal data that have not been 'notified' is a criminal offence. To help staff the College will provide copies of the College's 'notifications' under the DPA 1998, for reference in the College Library.

All staff are responsible for checking that any information they provide to the College in connection with their employment is accurate and up to date and that any changes at a later date are notified.

All staff are responsible for checking the accuracy of information held and keeping this information up to date.

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

Staff are responsible for ensuring that any person from whom personal data are obtained are not deceived or mislead as to the purpose for which such data are held, used or disclosed. Staff must ensure that an indication of the purpose[s] should appear on any form used to collect data, and where necessary, an explanation as to why the data are being collected. No unfair pressure should be used to obtain any personal data.

5.4 Student Responsibilities

Students must ensure that all personal data provided to the College are accurate and up to date. They must ensure that changes of address etc. are notified to the appropriate person normally their GST. Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify their personal tutor who will notify the data controller. Any student who requires further clarification about this should contact their personal tutor who will liaise with the Data Controller.

6.0 Data Security

All staff should observe strict control of all databases of information [computerised or manual] on living individuals, whether they be staff, students, members of the public, suppliers, customers etc. The College must 'notify' all relevant filing systems and databases or it could face legal action.

Failure of any member of staff to inform College management of the existence of a database or manual filing system could result in disciplinary action.

The holding of a College-related database outside the College also falls within these restrictions. The removal of College-Related personal data on a computer to off-site locations or the holding of College-related personal data on a computer outside College will only be permitted in strictly controlled circumstances. It is not permitted to hold any College-related data off-site on a computer or other "relevant filing system" without prior approval from college management.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Great care must be taken not to disclose personal data either intentionally or accidentally.

This can be helped by:

- Only allowing authorised access to computers [i.e. by not disclosing passwords]
- Logging off or locking computer systems when left unattended
- Keeping doors to rooms containing manual filing systems or computerised databases locked, when not in use
- Preventing unauthorised information being obtained from computer screens
- Not disclosing personal information over the telephone without following established procedures
- Only disclosing personal information to which an individual is entitled after first verifying the true identity of the person requesting the information
- Data must be encrypted before being transferred electronically. The Network Services team can explain how to send data to authorised external contacts.
- Staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Ensure proper disposal of waste materials such as computer printouts containing personal data
- Not removing any data/information from the college without prior authorisation

- Not storing/processing certain personal data on individuals unless it is absolutely required.
- Before processing any personal data, all staff should consider the following checklist:
- Do you really need to record the information?
- Is the information 'standard' or 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- Have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interest of the student/staff member to collect and retain the data?
- Have you informed the designated data controller for the College that you are storing this kind of information in a 'relevant filing system'?

7.0 Equality and Diversity Statement

Selby College welcomes and celebrates equality and diversity. We believe that everyone should be treated equally and fairly regardless of their age, disability, gender, gender identity, race, religion or belief, sexual orientation and socio-economic background. We seek to ensure that no member of the College community receives less favourable treatment on any of these grounds which cannot be shown to be justified.

This document is written with the above commitment, to ensure equality and diversity is at the centre of working life at Selby College.

8.0 Safeguarding Policy

Selby College recognises its moral and statutory responsibility to safeguard and promote the welfare of students. We work to provide a safe and welcoming environment where students are respected and valued. We are alert to the signs of abuse, neglect, radicalisation and extremism and follow our procedures to ensure our students receive effective support, protection and justice. Selby College expects Governors, staff and volunteers working on behalf of the college to share this commitment.

9.0 Fraud, Bribery & Corruption

Selby College follows good business practice and has robust controls in place to prevent fraud, corruption and bribery. Due consideration has been given to the Fraud Act 2006 and the Bribery Act 2010 in the development/review of this policy document and no specific risks were identified.

This document is designed for viewing through SharePoint. Printed copies, although permitted, are deemed uncontrolled. Please refer to SharePoint for the latest version (http://coffee).

APPENDIX A: SELBY COLLEGE: DATA SUBJECT ACCESS REQUEST FORM

TO: The Data Protection Officer [Selby College]
FROM: [For identification purposes only please provide]

FULL NAME:	
DATE OF BIRTH:	
ADDRESS + POSTCODE:	

In accordance with my rights under the GDPR, I [the above named person] wish to have access to the following data that the college may hold about me as part of an automated system or any other relevant filing system.

[Please tick as appropriate]

- ○ Personal details including name, address, date of birth, ethnicity etc.
- ○ Political, religious or trade union information.
- ○ Academic marks or course work details.
- ○ Academic or employment references.
- ○ Health and medical matters including learning difficulties and disabilities.
- ○ Disciplinary records.
- ○ Any statements of opinion about my abilities or performance.

Other data [Please specify]

Signed:	Date:

Note. In accordance with Selby College data protection policy the College aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within 30 days of request unless there is reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

APPENDIX B: GDPR Overview

GDPR applies to Selby College in that we are an organisation that stores and processes information about living individuals. Therefore all members of Selby College staff must adhere to data protection law.

Personal data must be:

- processed fairly and lawfully
- processed appropriately and must be for a specific limited purpose
- relevant and not excessive in relation to the purpose for which it is held
- accurate and up to date
- only kept for as long as is necessary
- processed in accordance with the rights of individuals under the act
- kept and in a secure manner
- only transferred to other countries who have equivalent data protection controls.

What data and filing systems are relevant?

All filing systems where we hold information about living individuals are regarded as relevant filing systems under the GDPR. This includes any filing system, not just computer systems, where information about individuals is readily accessible and includes data held in filing cabinets, folders, concertinas, card indexes, CCTV footage etc.

What do I do if I am holding information about individuals?

- Inform the College data protection officer [Mike Pilling, Network Services Manager] and read the College GDPR Data Protection Policy.
- If the data held are sensitive [Ethnic origin etc.] obtain express permission from the individual concerned to hold the data.
- Keep the data in a secure environment:
- Only allow authorised access to computers via password protection.
- Lock filing cabinets/offices.
- Do not remove data from the College without permission.
- Ensure proper disposal of old data.
- Do not store any data that you would not want an individual to see [Personal opinions etc] and only store what is absolutely necessary for purpose.
- Ensure that data is accurate [up to date].
- Be ready to provide copies of all data relating to an individual if requested by the data controller.
- Ensure that individuals understand why and how we process the data we do.

What rights do individuals [data subjects] have to see the data we hold about them?

One of principal objectives of the Data Protection Act (2018) is to create transparency and openness. Individuals have the right to see the data we hold about them and to understand how we use the data. Individuals can request to see the data we hold about them and under the law we have to provide access to their data [with only a few exceptions].