FE College Sector (NI)

GDPR Staff Handbook

NORTHERN Regional College

In partnership with:

South West College

belfast met "outstanding learning for successful futures"

SERC INSPIRING. TRANSFORMING. ENRICHING.

north west regional college Derry~Londonderry • Limavady • Strabane

src Southern Regional College

Contents

1 Introduction

The General Data Protection Regulations (GDPR) place obligations on all organisations to protect personal data by means of adequate organisational and technical measures.

The College must demonstrate accountability to meet the key provisions of GDPR and the mandatory Principles listed within Article 5 of GDPR:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

This handbook has been written to compliment the Data Protection Policy and serve as a reference tool to help you and your department demonstrate compliance with legislation

The College Data Protection Officer is available on dpo@nrc.ac.uk to provide additional advice and guidance in relation to any of the contents within this handbook or answer other data protection related queries you may have.

2 Confidential Waste

The College requires that measures be taken to store, access and dispose of personal/sensitive information appropriately to protect against unauthorised disclosure.

Unlawful disclosure is a breach of the 6th Principle of the General Data Protection Regulations:

“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')”

All staff must ensure that both, personally identifiable/sensitive, paper or hard copy documents are disposed of into confidential waste bags, bins or shredders provided across College campuses.

Individuals handling or processing any confidential material are personally responsible for ensuring the proper disposal of the information.
Staff must be vigilant to the fact that if such confidential information is not disposed of securely into the confidential waste bins the trust could be fined up to €20m or 4% of our global annual turnover (whichever is greater) by the Information Commissioners Office.

3 Consent

What is consent and why does it matter?

Consent is one of a number of "lawful basis for processing" under GDPR. Under GDPR consent is defined as:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him".

If the individual has no choice but to have their information processed, the consent is not freely given and would be considered invalid if challenged.

This introduces a number of changes to consent. If you rely on consent as a condition for processing then you will have to:

- Ensure the consent is clear and unambiguous (e.g. no pre-ticked opt-in boxes)
- Place consent declarations separate from other terms and conditions
- Provide clear and easy ways for subjects to withdraw consent at any time
- Retain records of consent throughout the lifetime of the data processing.

The other important aspect of consent under GDPR is that using it as a basis for processing open up additional rights for data subjects including:

- The right to erasure ("right to be forgotten")
- The right to data portability (to have their data provided in common electronic formats).

The Information Commissioner's Office (ICO) has indicated that public authorities will find consent difficult to justify as the basis for processing due to the power imbalance between the data controller and data subject and has recommended that, where possible, public authorities should not rely on consent as a lawful basis for processing.

If you rely on consent for processing personal data you should review your consent mechanisms and try and identify another lawful condition for processing the data if possible. See appendix 1 for other lawful conditions.

Special Category Personal Data

Where you need to rely on consent you will have to make sure that you meet the GDPR consent requirements.

Getting consent wrong can have serious consequences for the College, including the highest tier of administrative fines which can be given under GDPR, which could mean a fine of up to €20 million.

Children's Consent

Children's consent must meet all of the requirements (for consent) set out under GDPR.

The GDPR does not set a prescribed age at which children can give consent, however it does require any child giving consent for online services to be 16 or over, otherwise parental consent is required[1].

Special Categories of Personal Data

The GDPR refers to "sensitive personal data" under the DPA as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes including the addition of genetic data and biometric data.

If you process special category data on the basis of consent, then the GDPR sets a slightly higher standard of "explicit" consent. The GDPR does not define "explicit" but the ICO suggests that explicit consent must be affirmed in a clear statement such as "I consent to …" which also specifies the nature of the data and the processing that requires consent. You must therefore take additional care when wording your consent statements when dealing with special category data.

Identify the lawful basis for your processing

You must identify the lawful basis for processing personal data held by their business areas. (see appendix 1)

Processing which cannot be attached to a lawful basis should be halted as it is unlawful and a breach of the 1st Principle of GDPR.

---

[1] It also allows for Member States to reduce this age, but to no lower than 13 years old – draft Data Protection Bill shows UK opting for 13 years old.

Eliminate consent where possible

If you are currently using consent as a lawful basis for processing, consider whether another condition is relevant. Possible conditions for the College are:

Alternative lawful basis for processing	Description
A contract with the individual	Where you supply goods or services or enter into an employment contract.
Compliance with a legal obligation	Where you are required by UK or EU law to process the data for a particular purpose.
A public task	To carry out your official functions or a task in the public interest. The ICO view is that this is the legal basis for most activities of public authorities that fall within their official functions.

Note: Under the GDPR the "legitimate interests" condition for processing does not apply to public authorities if the processing is part of their core business function. Legitimate interest can only be used if the processing is in the interest of a third party.

If after assessing your conditions for processing you feel that you do need to rely on consent you should follow the more detailed guidance below.

4 Relying on Consent for Processing Personal Data

Actions to be followed

Obtaining consent

Where consent is agreed as the only lawful condition for processing, you will have to determine whether your processes meet the current GDPR standards. The ICO has developed a consent checklist, which sets out the steps you should take to seek valid consent under the GDPR. The checklist can also help you to review existing consent.

If you have difficulty meeting the standard for consent, it may not be the most appropriate basis for your processing, so you should consider another lawful basis for processing.

If your current means of obtaining consent meets the requirements of the GDPR then you are not required to obtain fresh consent.

If, as is likely, it does not meet the current GDPR standards, you will have to obtain new consent.

Key Changes to Consent under GDPR

Consent must be "unambiguous" and be "a clear affirmative action" by the data subject. The ICO sets out some key conditions for the use of consent: You will need to determine if your current means of obtaining consent meets these conditions.

Consent conditions	Description
Unbundled	• You must keep consent requests separate from other terms and conditions. • You cannot make consent a precondition of signing up to a service unless necessary for that service.
Active	• The subject must opt-in. You cannot use pre-ticked opt-in boxes or assume consent.
Granular	• The subject must consent separately to different types of processing wherever appropriate.
Silence	• Silence/no response must never be accepted as assumed consent.
Named	• You must make it clear to the subject which department they are giving consent to.
Documented	• You must keep records of what the subject consented to and how and when you obtained consent.
Easy to withdraw	• You must tell subjects they can withdraw consent and it must be as easy to withdraw as it was to give consent.

Additional Rights under GDPR

Under the GDPR individuals have rights including:

- To be informed about how you are processing their data
- To have access to their data
- To have their data rectified.

When you use consent as the basis for processing, the GDPR provides additional rights to individuals:

Right to erasure ("right to be forgotten")	• Where the person withdraws consent they can ask to have their data removed. This right has changed under the GDPR as under the DPA the processing had to "cause unwarranted and substantial damage or distress". This is no longer the case under GDPR.
Right to data portability	• The person has the right to obtain copies of data relating to them in common machine readable formats for transfer to themselves or other third party data controllers.

You will have to ensure that your processes are able to handle any requests "to be forgotten" and to provide individuals with their data in common formats.

Consent Checklist 

Action	Check
Asking for consent	
We have checked that consent is the most appropriate lawful basis for processing.	
We have made the request for consent prominent and separate from our terms and conditions.	
We ask people to positively opt in.	
We don't use pre -ticked boxes, or any other type of consent by default.	
We use clear, plain language that is easy to understand.	
We specify why we want the data and what we're going to do with it.	
We give granular options to consent to independent processing operations.	

Action	Check
We have named our organisation and any third parties.	
We tell individuals they can withdraw their consent	
We ensure that the individual can refuse to consent without detriment.	
We don't make consent a precondition of a service.	
If we offer online services directly to children, we only seek consent if we have age-verification and parental -consent measures in place.	
Recording consent	
We keep a record of when and how we got consent from the individual.	
We keep a record of exactly what they were told at the time.	
Managing consent	
We regularly review consents to check that the relationship, the processing and the purposes have not changed.	
We have processes in place to refresh consent at appropriate intervals, including any parental consents.	
We consider using privacy dashboards or other preference - management tools as a matter of good practice.	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.	
We act on withdrawals of consent as soon as we can.	
We don't penalise individuals who wish to withdraw consent.	

HIGHER LEVEL APPRENTICESHIP EMPLOYER CONTACT CONSENT FORM	NORTHERN Regional College

Dear Applicant

We would like your permission to use your personal data held by the College to contact prospective employers (name, contact details, date of birth, course and academic record).

We would like to contact employers for the following reasons relating to your application to a Higher Level Apprenticeship:

- ☐ Application for Apprenticeship
- ☐ Interview/Contact for Apprenticeship
- ☐ Progress on application

Your permission to contact prospective employers will only be used for the reasons you have ticked above and only for the academic year 2019/20.

Applicant Details	
Applicant Name	
HLA applied for	
Address	
Date of Birth	
Contact number	

College Contact Details	
College Staff	
Address	
Contact number	

I (the applicant) confirm I understand the purpose for which my data is being used and I give my permission for this to happen. I understand I may withdraw consent at any time by emailing DPO@nrc.ac.uk and my Rights are available on the **College website**. Until then, my information will be used until the end of 2019/20 and destroyed as per the FE Sector Retention and Disposal Policy.

Applicant Signature: …… Date: ……..

PARENT/GUARDIAN CONTACT CONSENT FORM	NORTHERN Regional College

Dear Student

We would like your permission to use your personal data held by the College to contact your parent/guardian (name, contact details, date of birth, course and academic record).

We would like to contact your parent for the following reasons relating to your progress on your course (student to tick the boxes staff are allowed to contact parent/guardian):

- ☐ Parent evening
- ☐ Academic Progress Reports
- ☐ Other please provide details (e.g. discipline, attendance)

Your permission to contact your parent/guardian will only be used for the reasons you have ticked above and only for the academic year 2018/19.

Student Details	
Student Name	
Student I.D. no.	
Address	
Date of Birth	
Contact number	

Parent/Guardian Contact Details	
Parent/Guardian Name	
Address	
Contact number	

I (the student) confirm I understand the purpose for which my data is being used and I give my permission for this to happen. I understand I may withdraw consent at any time by emailing DPO@nrc.ac.uk and my Rights are available on the **College website**. Until then, my information will be used until the end of 2018/19 and destroyed as per the FE Sector Retention and Disposal Policy.

Model/Profile Consent Form **Photographic, Film and Profile Permission**	NORTHERN Regional College

Thank you for agreeing to act as a model for photography and/or film, and/or for providing a written profile and/or quotes for the Northern Regional College. We intend to use the images and written profile, where appropriate, in our promotional material to tell others about the benefits of the College. We would like to use your photograph, film footage, profile and quotes in publicity which may appear locally, nationally and worldwide.

Please indicate which of the following places you consent to your image/profile being used. This is not a complete list of publicity channels, but is indicative of the types of location that the College uses for promotional purposes:

- ☐ Printed materials – e.g. prospectuses, brochures, posters
- ☐ Website
- ☐ Press
- ☐ Social Media
- ☐ Advertising e.g. digital, print and outdoor billboard

On occasion we work in partnership with external organisations to promote the Northern Regional College. Please indicate below if you give consent for your image/profile to be used in this way:

- ☐ External organisations

The College will keep your image/profile on our records for no more than three years. Your personal data will only be used and stored in accordance with GDPR legislation.

It is standard practice for a photographer/filmmaker to show their work online and/or printed portfolios and to share it via social media. Please indicate below if you consent to your image being used in this way:

- ☐ Photographer's use

I understand that I have the option to withdraw my consent by contacting the College's Data Protection Officer via email DPO@nrc.ac.uk

Privacy and Data Protection
At Northern Regional College we are strongly committed to protecting the privacy of your personal data, in whatever form that information is held. We will ensure your personal data is properly safeguarded and processed in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (collectively referred to as Data Protection Legislation).

You can view your rights and obligations via the College Website:
http://www.nrc.ac.uk/page/privacy-policy

Name:
Signature: Parent's signature (if applicable):
Student ID (if applicable):

5 Contracts

For the majority of personal data processing, the College is the 'Data Controller'.

GDPR places liability on both the Data Controller and the Data Processor therefore, there must be a contract in place where there is third party involvement in our data processing.

The ICO can fine one or both parties, depending on where the evidence shows data breach has occurred.

If there is a clear and unambiguous contract, it will then be clear to identify where the error has occurred should there be a data breach.

Assurance should be sought BEFORE a contract is awarded or signed. Due to the potential impact of a data breach, the College must be satisfied that a Data Processor agrees to the following – this should be explicit in any contract.

Contract checklist

Contract Requirement	Check
Observe Procurement Guidance Note PGN 01/18	
Only appoint Data Processors who provide sufficient data protection guarantees	
Have a binding contract in place which both parties have agreed and signed by both parties to include:	
• Nature of the processing activities	
• Act only on specific written instructions – be explicit about what the data processor can and cannot do i.e. use for purposes outside the College instructions	
• Ensure confidentiality is observed	
• Assurances of adequate security measures	
• The Data Processor must be able to assist the College with actioning data subject rights e.g. erasure, access, rectification	
• Can the data processor delete or return personal data either on demand or at the end of a contract	
• Processor cannot enlist a sub-processor or share with third party without the Colleges consent	
• Contract data protection requirements are passed to the sub-processor where employed	
• Data Processor must allow the Data Controller to periodically audit their processing	
Data Processor staff who will be engaging with College data are fully trained and aware of their data protection responsibilities	

Organisations must not accept any cost which may arise in order for a Data Processor to meet GDPR requirements	

6 Data Breach

The College has an obligation to notify the ICO in relation to any personal data breaches. Article 33 states that each Data Controller must notify without undue delay and no later than 72 hours after becoming aware of the breach.

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Each staff member has an obligation to report all suspected or confirmed personal data breaches **immediately** to the College Data Protection Officer as per the **Data Breach Management Procedure.**

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, the College must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then the College must notify the ICO; if it's unlikely then the College does have to report it to the ICO.

The DPO will make a decision on the severity of the breach and follow the procedure accordingly.

The College will contain the breach and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

All information and communications in relation to data breaches should be well documented.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to €10 million or 2% of global turnover. The fine can be combined with the ICO's other corrective powers under Article 58.

It is therefore important that we follow our robust Data Breach Management Procedure to ensure we detect and can notify a breach, on time; and to provide the necessary details.

7 Data Sharing Agreements

Required when entering an agreement that will require data to be shared between parties systematically

- Be clear on what the purpose of sharing the data
- Assess the potential benefits and risks to data subject(s) of sharing/not sharing
- Is the sharing proportionate to the purpose of the data sharing?
- Could the purpose be achieved without sharing?

Do you have the authority to share?

- Are there necessary functions that require data to be shared?
- What the data you wish to share given in confidence?
- Are there legal obligations that require data to be shared?

If you decide to share:

It is good practice to have a data sharing agreement in place that should consider the following:

- What information needs to be shared?
- What organisations are involved?
- What do you need to tell data subjects whose information will be shared? How will this be communicated?
- What measures are in place to ensure adequate security to protect data?
- What procedure is in place for data subjects to access their personal data if requested?
- What is the retention period for the data?
- What procedures are in place to ensure secure deletion takes place?

Data Sharing For One Off Requests

When requested to share personal data in ‘one off’ circumstances

Consider the following key points:

- Why should the data be shared?
- What are the potential benefits and risks to the data subject(s) of sharing/not sharing?
- Any concerns that a data subject is at risk of serious harm?
- Do exemptions apply?

Do you have the authority to share?

- Are there necessary functions that require data to be shared?
- What the data you wish to share given in confidence?

- Are there legal obligations that require data to be shared?

If you decide to share:

- What information needs to be shared? Only share what is necessary.
- Distinguish fact from opinion.
- How will the information be shared?
    - What security will be used?
    - Will the authorised personnel receive it?
    - Do you need to inform the data subject that you are sharing their information?

Record your decision:

Record your data sharing decision and your reasoning – Yes/No

If sharing information, record the following:

- What information was shared and for what purpose?
- Who it was shared with?
- When it was shared?
- Why it was shared?
- Was consent given to share the information? – Yes/No

8 Disposal of Records

Under the GDPR, data controllers (i.e. businesses using personal data,) should not retain personal data for any longer than necessary. Furthermore, the GDPR gives data subjects rights to require the erasure of their personal data (also known as “the right to be forgotten”).

Minimising data retention and having clear procedures in place to determine how and when to dispose of personal data is therefore key to complying with the GDPR. Not only that, but a well-managed data retention plan can help the College to avoid the information overload and high storage costs resulting from the retention of unnecessary (and often redundant) data.

The retention of unnecessary paper and electronic records consumes staff time and utilises space and equipment. Records management is ultimately a matter of risk management, and the College must determine their own position on managing the risks associated with the retention and disposal of records.

To assist in this process a Data Retention and Disposal Policy should set out the limits that apply to the various types of personal data held by the College; to establish the criteria by which those limits are set; and to set out how personal data should be deleted or disposed of.

The FE Sector has collaborated on the development of a single **Retention and Disposal Schedule** for all the Colleges. The creation of the document has been supervised by the Public Record Office for Northern Ireland (PRONI). The purpose of this Retention and Disposal Schedule is to manage the life of records from their creation to their completion. The Retention and Disposal Schedule will identify records of historical value and determine whether they are to be preserved as archives, either by the Colleges or PRONI and records which are to be destroyed. It provides guidance on retention of the records which are generated by the Colleges in the course of carrying out their functions and managing the Colleges as corporate bodies.

Decisions to preserve or destroy records should be in line with the Sector Retention and Disposal Schedule if you are unsure as to what to hold or destroy please seek advice for the Data Protection officer in the first instance.

Note:

Should you keep personal data documents longer than retention dates, you are in in breach of the College Data Protection Policy. Should the College receive a data subject access request, you will be required to disclose this information by law.

9 Good Housekeeping

We are all encouraged to ensure good housekeeping when handling information and data. In line with the data protection legislation and best practice organisations are required to dispose of out-of-date information, freeing up both physical and computerised filing systems and making valuable information easier to find.

Everyone is therefore encouraged to treat personal data with respect – following the Colleges Data Protection Policy and associated procedures will create a general level of awareness of personal data issues, helping to ensure that information about our staff students and partners is treated properly.

To assist us all in this obligation there are a number of good housekeeping tips that we all should follow:

Your work area

- **Keep a tidy desk –** ensure that you adopt a clear desk policy as not only is it important to keep your work area tidy from a health and safety point of view it is also important in protecting information and data. It enhances security in that as passwords and information get locked away
- **Reduce the amount of paper you keep –** many people often retain copies of documents as some form of back up for their own "peace of mind" - in case information is lost –if you are unsure whether papers should be kept then it is probably better that you dispose of it correctly "if in doubt you should throw it out"
- **Do not print off emails to read them –** this generates unnecessary amounts of paper which increases the risk of potential loss of data or of emails becoming attached to other documents inadvertently. Adopt the approach of handling papers only once and act on it, file it or dispose of confidentially or shred. Consider scanning papers to your PC and storing them correctly if you are required to keep them.
- **Position you PC away from windows or visitors** into your building or office to prevent accidental disclosures of personal data.

Staff Areas

- Do not leave material containing personal data in a visible area.
- Remember to check pigeon holes, photocopiers, printers.

Forwarding Emails

- When you forward an email to others or copy new people into an email thread review the content in the entire email and ensure the information contained is suitable for everyone receiving it.
- It is very easy to forward emails to others not realising there is content within it that others should not have access to.

Security of College Devices

- College devices such as smart phones, laptops and pen drives should not be left unlocked or unattended. Ensure they are out of sight whilst in transit or off site.

Encrypting Personal or Sensitive data

- If you are required to send sensitive or personal data to an external source ensure that you send this information in an encrypted manner.
- Do not store or hold personal or sensitive data on unsecured smartphones, laptops and pens drives. Log off or lock your workstation each time you leave it.

Discussions

- It is easy to forget when discussing business with Colleagues, especially sensitive or personal information, that others may be able to overhear your conversations if they are within the vicinity.
- If you need to hold this type of conversation, then agree to hold off the conversation until you are able to hold it in a more confidential space.

10 Overseas Data Sharing

Transfer of personal data outside the European Union, to third countries or international organisations is restricted under GDPR regulations. This is to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

For full details refer to Chapter V of GDPR - https://gdpr-info.eu/chapter-5/

Overview

'Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.'

Safeguards

Personal data may be transferred if the organisation receiving the data has provided adequate safeguards such as:

- a legally binding agreement between public authorities or bodies
- binding corporate rules (agreements governing transfers made between organisations within a corporate group)
- standard data protection clauses in the form of template transfer clauses adopted by the Commission
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission
- compliance with an approved code of conduct approved by a supervisory authority
- certification under an approved certification mechanism as provided for in the GDPR
- contractual clauses agreed authorised by the competent supervisory authority
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Transfers based on an organisation's assessment of the adequacy of protection

Personal data transfers based on your own assessment of the adequacy of the protection afforded to the personal data is limited under GDPR.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Are there any derogations from the prohibition on transfers of personal data outside the EU?

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request
- necessary for the performance of a contract made in the interests of the individual between the controller and another person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register)

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Data Transfers For One Off Requests

If it is not possible to demonstrate that the data subject(s) rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers
- is not repetitive (similar transfers are not made on a regular basis)
- involves data related to only a limited number of individuals
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual)
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data
- In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals

11 Privacy Notices

What is a Privacy Notice?

The first Principle of GDPR (Transparency) states:

“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”

You cannot be fair if you are not being honest. Individuals must have a reasonable expectation of what the College is doing with their information.

A Privacy Notice is the most open and honest method of telling individuals why you are collecting their personal information and what you intend to do with it. This is now a legal requirement and the College must be able to demonstrate its transparency to individuals and the ICO in the event of an investigation.

When do I need a Privacy Notice?

They should be provided:

- at all points of data collection
- at the earliest opportunity and without delay
- Where there is a previously unforeseen processing activity which has not been previously communicated

Privacy Notices must be:

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

Examples of where to provide a Privacy Notice

You may wish to consider providing a Privacy Notice on any of the following, whichever is applicable:

Website, footer of a form which individuals are asked to complete with personal information, online ‘?’ icons, leaflets, newsletters, staff handbook, contracts of employment, student portal, CCTV signage, signatures on emails, template letters.

Privacy Notice Checklist 

The College has an overarching Privacy Notice on its website however where you are gathering personal data from either the individuals themselves or a third party, you **must** provide the following information where appropriate:

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained.	• Within a reasonable period of having obtained the data (within one month) • If the data are used to communicate with the individual, at the latest, when the first communication takes place; or • If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

12 Data Protection Impact Assessments

Under the GDPR, the College has a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities

Data Protection Impact Assessments (DPIAs) is a tool which can help the College identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow the College to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

DPIA's must be completed and signed off BEFORE a project is agreed. The DPO must be consulted at the earliest opportunity to assist and advise with the DPIA.

The DPIA template is held by the DPO and a copy should be requested directly.

When is a DPIA required?

You 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.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.

- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project

Who should be involved?

The Head of Department/ or Manager should complete the DPIA.

Recording the findings

All DPIA's should be thoroughly completed in the event of College processing activities and decisions being challenged.

The Data Protection Officer will hold a recording of all the outcomes of the DPIAs.

Consultation with the ICO

If the DPIA finds the processing is "likely to result in a high risk to the rights and freedoms of natural persons", and the College is unable to mitigate against the risk, the Data Protection Officer is required to consult the ICO (Supervisory Authority) before conducting the activity.

There may be an Exemption by mitigation and possible restriction by ICO.

13 Removing Personal Identifiers

Anonymisation

Anonymisation is a valuable tool that allows data to be shared, whilst preserving privacy. The process of anonymising data requires that identifiers are changed in some way such as being removed, substituted, distorted, generalised or aggregated.

A person's identity can be disclosed from:

- **Direct identifiers** such as names, postcode information or pictures
- **Indirect identifiers** which, when linked with other available information, could identify someone, for example information on workplace, occupation, salary or age

You decide which information to keep for data to be useful and which to change. Removing key variables, applying pseudonyms, generalising and removing contextual information from textual files, and blurring image or video data could result in important details being missed or incorrect inferences being made.

Anonymising research data is best planned early in the research to help reduce anonymisation costs, and should be considered alongside obtaining informed consent for data sharing or imposing access restrictions. Personal data should never be disclosed from research information, unless a participant has given consent to do so, ideally in writing.

Data masking

This involves stripping out obvious personal identifiers such as names from a piece of information, to create a data set in which no person identifiers are present.

Variants:

- Partial data removal – results in data where some personal identifiers, eg name and address have been removed but others such as dates of birth, remain.
- Data quarantining - The technique of only supplying data to a recipient who is unlikely or unable to have access to the other data needed to facilitate re-identification. It can involve disclosing unique personal identifiers – eg reference numbers – but not the 'key' needed to link these to particular individuals.

These are relatively high risk techniques because the anonymised data still exists in an individual-level form. Electoral roll data, for example, could be used to reintroduce names that have been removed to the dataset fairly easily. However, this type of data

is also relatively ‘rich’ in terms of allowing an individual to be tracked as part of a longitudinal study for example.

Pseudonymisation

De-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified.

Deterministic modification is a similar technique. ‘Deterministic’ here means that the same original value is always replaced by the same modified value. This means that if multiple data records are linked, in the sense that the same name (or address, or phone number, for example) occurs in all those records, the corresponding records in the modified data set will also be linked in the same way. This facilitates certain types of data analysis.

This is also a relatively high risk technique, with similar strengths and weaknesses to data masking.

Aggregation

Data is displayed as totals, so no data relating to or identifying any individual is shown. Small numbers in totals are often suppressed through ‘blurring’ or by being omitted altogether.

Variants:

- Cell suppression - if data is from a sample survey then it may be inappropriate to release tabular outputs with cells which contain small numbers of individuals, say below 30. This is because the sampling error on such cell estimates would typically be too large to make the estimates useful for statistical purposes. In this case, suppression of cells with small numbers for quality purposes acts in tandem with suppression for disclosure purposes.
- Inference Control – Some cell values (eg small ones such as 1-5) in statistical data can present a greater risk of re-identification. Depending on the circumstances, small numbers can either be suppressed, or the values manipulated (as in Barnardisation). If a large number of cells are affected, the level of aggregation could be changed. For example, the data could be linked to wider geographical areas or age-bands could be widened.
- Perturbation – such as Barnardisation - is a method of disclosure control for tables or counts. It involves randomly adding or subtracting 1 from certain cells in the table. This is a form of perturbation.

- Rounding – rounding a figure up or down to disguise precise statistics. For example if one table may have a cell with value of 10,000 for all people doing some activity up to the present date. However, the following month, the figure in that cell rises to 10,001. If an intruder compares the tables it would be easy to deduce a cell of 1. Rounding would prevent this.
- Sampling - in some cases, when very large numbers of records are available, it can be adequate for statistical purposes to release a sample of records, selected through some stated randomized procedure. By not releasing specific details of the sample, data holders can minimise the risk of re-identification.
- Synthetic data - mixing up the elements of a dataset – or creating new values based on the original data - so that all of the overall totals and values of the set are preserved but do not relate to any particular individual.
- Tabular reporting – a means of producing tabular (aggregated) data, which protects against re-identification.
- These are relatively low risk techniques because it will generally be difficult to find anything out about a particular individual by using aggregated data. This data cannot support individual-level research but can be sufficient to analyse social trends on a regional basis, for example.

Derived data items and banding

Derived data is a set of values that reflect the character of the source data, but which hide the exact original values. This is usually done by using banding techniques to produce coarser-grained descriptions of values than in the source dataset eg replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form.

Again, this is a relatively low-risk technique because the banding techniques make data-matching more difficult or impossible. The resulting data can be relatively rich because it can facilitate individual-level research but presents relatively low re-identification risk.

14 Survey Guidance

Student surveys and feedback are essential for continuous improvement in the teaching and support services that we offer as a College. Through online surveys and focus groups, the College can generate data from students and customers in a very easy way. It is advised not to collect personal or special category data within a survey, surveys should be anonymised where possible. An email address is personal information so if you plan on collecting it you need to explain your reason for collecting it.

It is essential that when carrying out surveys that we comply with the data protection legislation and the following key points must be followed when conducting your survey;

- clearly explain the exact purpose as to why you care carrying out the survey
- establish the information that you need to collect – do not collect information that is not necessary
- explain how you will handle the data that you collect and who you plan on sharing the data with
- provide the student with an option to opt out
- you should not pass individual responses onto a third party without the student consent
- direct students to the College's overarching Privacy Notice that will provide further guidance on their individual rights including their right to complain

These points should be clearly explained within a privacy notice on any online or paper surveys.

If you are carrying out focus groups, this privacy notice can be explained verbally with recipients being given the opportunity to sign a sheet confirming their consent to participate in the survey and that they understand the above. You should retain a copy of the surveys and consent documentation and dispose of it in line with the FE Retention and Disposal Schedule.

You must make it absolutely clear that the individual responses will remain confidential, although the results of the survey may not be. If you collect any personal or special category data, you must make it very clear what you will use it for and the lawful basis for processing this information. Explicit consent is required if you are collecting special category data and you must retain a copy of the signed consent for each recipient.