SERC
INSPIRING. TRANSFORMING. ENRICHING.

SOP NUMBER: 249-05-2018
ACADEMIC YEAR: 2021/22 ONWARDS
DATE OF THIS ISSUE: OCTOBER 2021

TITLE:

Data Protection Handbook SOP

Summary of Contents:

In compliance with legislation and in line with the College Data Protection Policy this Standard Operating Procedure (SOP) provides staff with guidance in relation to various data processing activities.

Date First Created:
May 2018

Latest CMT Approval Date:
3 Nov 2021

Responsible Owner(s):

Information Officer

REVIEW INFORMATION

Reviewed: January 2019
May 2019
August 2019
May 2020
July 2021

Review Due: May 2022

Requires CMT Approval (yes/no): Yes

Previous Reference (for control purposes): N/A

FE College Sector (NI)

Staff Handbook

Contents

1 Introduction

The General Data Protection Regulations (UK 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 UK GDPR and the mandatory Principles listed within Article 5 of UK 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 UK 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 of procedures 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

2 Scope

This Standard Operating Procedure applies to SERC staff and authorised third parties which can include temporary staff and work experience candidates. Within this procedure, all authorised users are included in the term 'staff'.

It is the responsibility of each individual or team to assess the risks when processing data.

The College Data Protection Officer is available on informationrights@serc.ac.uk or ext 2862 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.

3 Archiving and Storage

As a Non-Departmental Public Body, the College is subject to Freedom of Information and Data Protection legislation which allow the public, staff and students the right to request information held by the College. As such it is critical that the College manages its records efficiently and takes steps to ensure all records are easily accessible and available. Legislation stipulates strict timeframes for responding to these requests

Departments and Schools must dispose of all documentation where the retention period has now lapsed. It is not necessary to do this check continuously. It is sufficient to check documents on a 6 – 12-month basis.

Information which must be kept for a determined period of time should be archived. See Section 5.0 of this SOP.

Staff should refer to Retention and Disposal Schedule when deciphering what documents should be archived or disposed. The entire schedule should be checked due to documents which cross reference between departments.

The Schedule will also indicate the length of time a document should be archived before destruction.

The following storage areas should be checked to manage all necessary information, whether for disposal or archiving:

- Offices/storerooms
- SharePoint/Team Sites
- Databases e.g. QL/TMS
- 'S' drives
- 'M' Drives
- Filing cabinets
- Drawers
- Shelving Units
- Mobile devices e.g. USB pens

Documents which have superseded their timeframe should be destroyed in line with their Confidential Waste procedures within this SOP.

3.1 Packing Storage Boxes

Once a department had decided which documents should be archived and sent to storage, they should arrange for these items to be packed into boxes.

Items should be packed in a methodical manner which will allow ease of retrieval and disposal at a later date. It will not be possible to visit the boxes once they are in storage and there is a cost for retrieval therefore staff must note what items are in each container to ensure the correct box is being recalled if necessary

Documents being sent to the offsite storage facility must be packed into boxes supplied by the service provider. Other box types will not be accepted

Boxes can be requested from the Records Manager. Details should include:

Archiving is for documentation only. At no time should the following items be packed into storage boxes:

- Empty lever arch/ring binder files
- Polypockets
- Elastic Bands
- Cash
- Desk items such as stationary, pen holders, staplers

Records with varying disposal dates should not be placed in the same box. Contents of each box should all have matching disposal dates.

3.2 Box Labelling

It is important all boxes are labelled in a consistent format

- Details which must always be recorded on the box are:
- Department: e.g. Finance/Student Funding
- Contents: e.g. 2015/16, Hardship applications, A-D
- Disposal date: e.g. 30/06/2023

Boxes and labels are available from the Records Manager. The labels must be put on each box as they contain barcodes which identify that box specifically.

Boxes which are being sent via courier to SERC archives should have the lids taped to the main container.

3.3 Arrange a box for collection

Once a box have been packed and is ready for collection, staff must ensure all boxes details are documented with the following list used as a minimum:

- Date sent to storage
- Storage facility e.g. SERC Archives/Oasis
- Department: e.g. Finance/Student Funding
- Contents: e.g. 2015/16, Hardship applications, A-D
- Disposal date: e.g. 30/06/2023
- Destroyed: Yes/No

A spreadsheet containing these details should be stored centrally on the Data Protection/FOI Teamsite.

Once complete, staff should notify the Records Manager who will arrange for the appropriate collection with Oasis/courier.

4 Confidential Waste

The General Data Protection Regulations (UK GDPR)/Data Protection Act (2018) requires that measures be taken to store, access and dispose of sensitive information appropriately to protect against unauthorised disclosure.

The 'Confidential Waste SOP' requires all staff to ensure that both, personally identifiable or organisationally sensitive, paper or hard copy documents are disposed of into confidential waste bins provided to all departments across SERC campuses.

Staff must be vigilant to the fact that if personal information is not disposed of securely into the confidential waste bins/bags provided, the College could be fined up to €20m or up to 4% of the College global annual turnover by the Information Commissioners Office.

Likewise, the unauthorised disclosure of commercially sensitive information, which is normally exempt from disclosure, could prejudice the College commercial interests and cause competitive harm.

All staff have a responsibility to consider security when disposing of information in the course of their work. Individuals handling or processing any confidential material are personally responsible for ensuring the proper disposal of the information.

4.1 Hardcopy Information

Even when paper is thought not to contain personally identifiable information, a check should be made to the document does not contain personal/commercially sensitive information.

Information of this type must be disposed of either by shredding or disposal in confidential waste bags/bins.

In the first instance, the above information should be disposed of in the confidential waste bins which can be found at various locations throughout the College campuses.

Confidential waste bags should only be used if one of the following criteria apply:
1. The bag will be filled and returned to Estates at the end of that same working day
2. The bag will be securely locked away at the end of each working day

Confidential waste bags are available from SERC Estates Department (Bangor/Ards/SPACE Campuses) or GFM (Lisburn/Downpatrick/Ballynahinch/Newcastle Campuses)

It is the staff responsibility within departments/staff working areas to notify Estates Department/GFM once the confidential waste bag is full and a new one required. Estates will arrange for its collection and issue a new one.

<u>Under no circumstances should:</u>
1. Personal/commercially sensitive information be disposed of in ordinary waste paper bins or recycle bins (blue bins).
2. Confidential waste bags should not be left in corridor areas for collection. Notify Estates/GFM of which room the bag is in and they will arrange pick up.

SERC has a contract with an external waste contractor who will shred the confidential bag contents. This process is on a request basis, depending on volume.

4.2 Electronic Information

When returning SERC issued devices, it is the responsibility of the staff member to whom it was on loan to delete documents/information which they have stored on that hard drive. Upon receipt, the ICT Department will then wipe any existing data to ensure no previous files are accessible to future users.

In the event of SERC disposing of hardware, an approved tender company will remove old hardware and cleanse all machines as per tender agreement.

Departments are responsible for identifying which documents should be retained / transferred to the archive rather than being disposed of as per the Retention and Disposal Schedule.

5 Consent

What is consent and why does it matter?
Consent is one of a number of "lawful basis for processing" under UK GDPR. Under UK 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 UK 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.

5.1 Special Category Personal Data

Where you need to rely on consent you will have to make sure that you meet the UK 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 UK GDPR, which could mean a fine of up to €20 million.

5.2 Children's Consent

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

The UK 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].

[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.

5.3 Special Categories of Personal Data

The UK 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 UK GDPR sets a slightly higher standard of "explicit" consent. The UK 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.

5.4 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 UK GDPR.

5.5 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 UK 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.

5.6 Relying on Consent for Processing Personal Data, Actions to be followed

5.6.1 Obtaining consent

Where consent is agreed as the only lawful condition for processing, you will have to determine whether your processes meet the current UK GDPR standards. The ICO has developed a consent checklist, which sets out the steps you should take to seek valid consent under the UK 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 UK GDPR then you are not required to obtain fresh consent.

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

5.6.2 Key Changes to Consent under UK 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.

5.6.3 Additional Rights under UK GDPR

Under the UK 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 UK 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 UK GDPR as under the DPA the processing had to "cause unwarranted and substantial damage or distress". This is no longer the case under UK 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.

5.7 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 do not 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.	
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.	

CONSENT FORM	College Logo

DEPARTMENT:_____

We would like your permission to use the following data about you:

Data controller should notify the various categories of data to be used e.g. name, contact details, image, opinion…

for the following purposes:

Purpose must be explicit, clear, and unambiguous to ensure transparency and the decision of the individual being informed. The individual must be informed of who the data will be shared with (if applicable) for what reason.

Title

First Name

Surname

Address

Date of Birth

Contact number

I 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 and details of this and my Rights are available on the College website https://www.serc.ac.uk/customer-privacy. Until then, my information will be used until the process is concluded and destroyed as per the FE Sector Retention and Disposal Policy.

Your Signature: **Date:**

6 Contracts

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

7 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.

7.1 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 Security Breach Management SOP.**

7.2 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 is unlikely then the College does have to report it to the ICO.

The DPO will decide 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.

7.3 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 in place to ensure we detect and can notify a breach, on time; and to provide the necessary details.

8 Data in Transit

As a data processor the College is responsible for carrying out its daily functions while complying with the General Data Protection Regulations (UK GDPR)/Data Protection Act (2018) and its 6 principles.

Article 5.1(f) of UK GDPR states:

> *"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')'*

SERC must ensure that all personal data is treated with appropriate security measures by all who handle it. 'Appropriate' is not defined in terms of hard and fast rules but is meant to urge a degree of precaution and security proportionate to the data type and the potential impact of unauthorised disclosure. It is not possible to implement precautions and actions to cope with all circumstances and conditions, therefore staff handling personal data must assume '*personal responsibility'* and make considered judgements in terms of how they handle data in their possession and when deciding for its transport from one secure location to another.

Due to the geographical division of SERC campuses and the nature of College operations it is necessary for the College to issue guidance in relation to the transit of personal data to include both hardcopy and electronic format.

This Standard Operating Procedure outlines the process all staff must refer to when arranging for the transport of personal data from one location to another.

Loss of personal data has substantial risk of causing harm/distress to the data subject and reputational damage to the College.

The risk of data being lost or damaged is at its highest when it is moved from its normal secure location to another location e.g. transit from one campus to another.

It is the responsibility of each individual or team to assess the risks when deciding which means to use for the transfer of data. This procedure will assist; however, it is not possible to provide guidance for every scenario. Each case needs to be considered on an individual basis.

If there is uncertainty in relation to what is deemed to be appropriate security measures in relation to the transport of data, the individual must contact the SERC Information Officer or his/her line manager for guidance.

The terms 'personal', 'confidential' and 'sensitive' data relate to all types of data covered by UK GDPR/Data Protection Act (2018).

Transport methods include:

- Internal Courier Service
- Post (incoming and outgoing)
- Personal transportation
- Scan
- Fax
- Email and other electronic means

If personal data is required to be sent from one secure location to another, the following principles must be considered before any action is taken:

Principle 1: Justify the purpose for sending personal data
Principle 2: Is its transport absolutely necessary
Principle 3: What is the minimum I can send / only send relevant data
Principle 4: Who should have access to this, what measures can I take to ensure this is not compromised
Principle 5: Recipient should understand their responsibilities in relation to keeping this data secure upon receipt
Principle 6: Understand and comply with the law – Data Protection Act (2018)

Arrangements for the transport of personal data should be relevant to:

- Data Format
- Volume of data to be transferred
- Level of risk re loss of data
- Urgency of the data transfer

Where data sharing protocols and agreements may already be in place for some service areas (e.g. DEL and Examination bodies) staff must act in accordance with the security standards specified in such agreements where they exceed those of the Data in Transit procedure. In all other respects staff must work to the standards set out in the Data in Transit SOP.

8.1 Modes of data transit:

8.1.1 Internal Courier

Anyone wishing to use this service for the transport of their own personal data e.g. sending documents or application forms to Human Resources/Finance does so at their own risk. It is the senders' responsibility to ensure urgent/official documents are sent by the most secure and timely means as possible. Loss of such documents can cause extreme inconvenience and result in considerable cost to replace. **The College will not accept responsibility for loss of personal documents sent via the courier facility.** All staff are responsible for updating their profile to reflect the Campus where they are based or where they wish their mail to be delivered.

- The Internal Courier Service operates twice weekly – Times and collection point details are available from Estates.
- There may be occasions when the courier services will be cancelled however where possible staff will be given 24hours notice to allow them to make other arrangements.
- Each main campus (Bangor, Lisburn, Downpatrick and Ards) has an allocated collection/delivery point at Customer Services. The collection/delivery point in Ballynahinch is within Human Resources.
- Staff who are willing to send personal data via the Internal Courier System should go to Customer Services and place their mail in the correct tray.
- Customer Services staff will then group mail according to destination and it will be placed in a sealed bag.
- Staff arranging for the removal of 'student' data e.g. enrolment forms, must note the type of document being moved e.g. student name/section of the alphabet, ensure the documents are secure and agree for its receipt to be confirmed by a colleague at the destination.

8.1.2 Post (Incoming)

It is also the responsibility of each staff member to provide their correct correspondence address to external contacts.

- *Royal Mail deliver* to the Bangor, Lisburn, Downpatrick, Ballynahinch, Ards, Ballynahinch, Holywood and Newcastle campuses on a daily basis.
- SERC will be given notice of any changes to service during holiday periods.
- Upon receipt of incoming mail, it will be date stamped and allocated to the correct fixtures on each campus for collection.
- It may be necessary for Customer and Community Services to open mail if the recipient details are unclear. If this happens, a Senior Customer Services Officer or nominee will open the mail.
- All post fixtures should be checked regularly for mail.
- At no point should mail be collected by anyone other than the recipient unless this is a School Support Officer, PA or appointed member within an office.

8.1.3 Post (Outgoing)

- *Whistl collect* from the Bangor, Lisburn, Downpatrick, Ballynahinch, Ards and Ballynahinch campuses on a daily basis.
- SERC will be given notice of any changes to service during holiday periods.
- Staff are responsible for ensuring accuracy regarding the recipient's name and destination address.
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery.
- Do not send the original copy of personal data where avoidable. If this is unavoidable, please arrange for this to be sent 'Recorded Delivery'.
- If desired, arrange for an email from the recipient to acknowledge receipt of the item.

8.1.4 Email

- Email is now a routine method of transporting information from one location to another.
- It is the senders' responsibility to ensure the recipients email address is up to date and keyed correctly to avoid delivery to an unauthorised third party.
- If forwarding an email, check that all information contained in previous emails is relevant to the new recipient.
- When emailing a group of people, using their *personal email* addresses i.e. non-SERC generated, please key their details into the **'bcc'** field. By doing this, each recipients detail are invisible to the others and therefore protected from unauthorised disclosure.
- If sending emails to external parties containing attachments containing personal data of more than one person e.g. spreadsheets, please apply a secure method of transfer in the event of interception e.g. 7Zip passwords (See diagram 1). The password should be included in a follow up email. Never send the password in the email containing the document.
- Alternatively, staff may also share a document via One Drive and email the password to the recipient
- Where a letter has been issued to an individual in the post, it would be acceptable to scan this communication to him/her without applying this method of security.

8.1.5 Scan

- When scanning documents to a recipient, staff must ensure the correct recipient is displayed on the screen of the copier before committing to send.
- Papers must be collected and removed from trays before staff leave the scanning machine,

8.1.6 Paper Records (hardcopy)

- Before taking personal information in non-electronic (paper) format, consider if there are other options available e.g. upload onto SharePoint, One Drive or scan.
- By removing hard copy documents from their normal secure location, staff are accepting accountability for their security and their contents to remain confidential against unauthorised access.
- On any occasion when work is brought home, at no point should personal data be left in plain sight e.g. in the car or hallway.

8.1.7 PC/laptop/non-SERC equipment

When working at home on a personal PC or laptop:

- Never work on SERC related personal data on a public device e.g. internet café/public library.
- Ensure personal data is stored correctly and securely i.e. on SERC regulated storage facilities – SharePoint.
- Never store/transfer personal data to a home PC or laptop or any other non-SERC device e.g. USB memory sticks, clouds.
- Only have as much personal information open as necessary and only for as long as necessary.
- Do not leave the computer unattended for any period of time such that others can access any personal data; always lock the computer or log out when not in use.
- Never leave a laptop in a car.

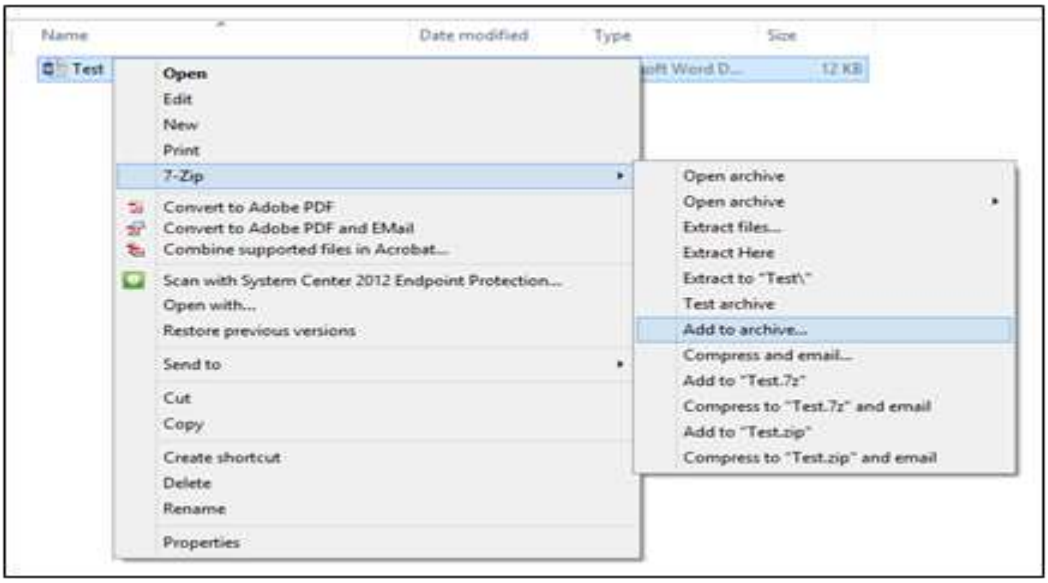
8.1.8 Fax

- Staff must not transfer any data via fax

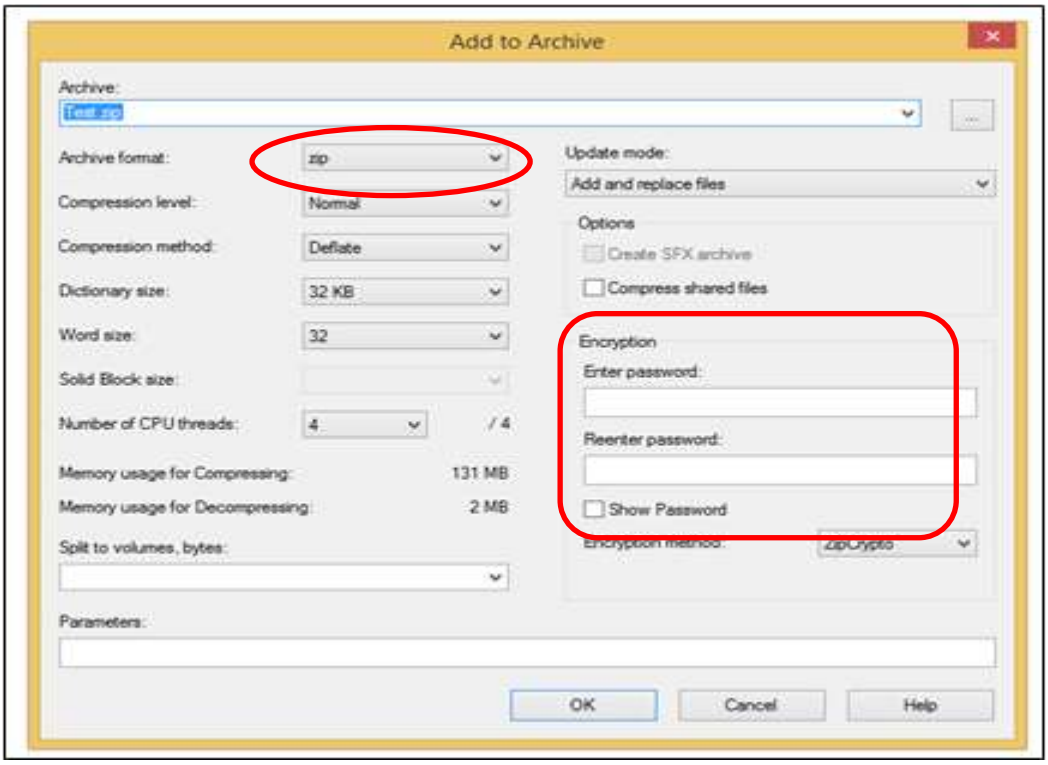
DIAGRAM 1

Guidance for applying 7Zip to a file

- Right click on the folder you want to password protect in an email
- Hover the cursor on 7Zip and a new menu will appear to the right
- Click on ‘Add to Archive’

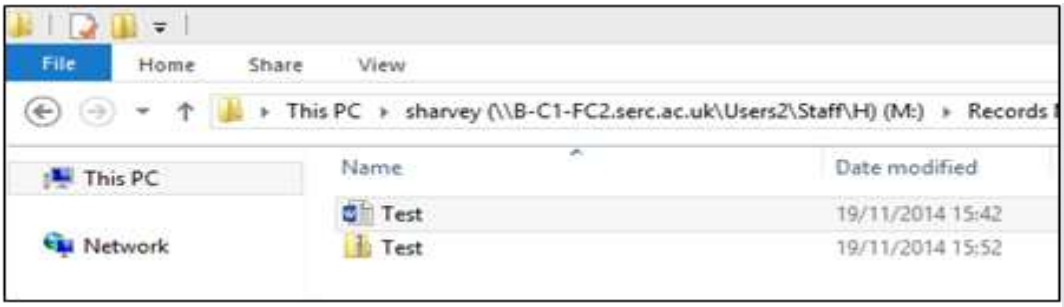


- Once you have that complete you will see the following



- Archive Format to ‘Zip’
- Enter a password of your choice which you will be sending to the recipient and re-enter
- Click ‘ok’
- Your file will now appear as a Zip folder.

This is the folder you select to send as your email attachment



Do not send the password in the same email as your document.

9 Data Protection Impact Assessment

Under the UK 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) are 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. It will also evidence the College considering the risks of a project/function should we be challenged.
Failure to carry out a DPIA risks a lower tier monetary penalty i.e up to €10m or up to 2% of the Colleges global annual turnover (whichever is greater)

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.

9.1 When is a DPIA required?

Article 35 of GDPR enforces organisations to carry out a DPIA when the processing has privacy implications such as:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals such as their data protection rights.

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).

** A "risk" is a scenario describing an event and its consequences, estimated in terms of* severity and likelihood.

The following 9 criteria should be used as an indication of a DPIA being required:

Criteria	Example
Evaluation/Scoring	profiling and predicting especially *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements"* It may include an organisation building behaviour patterns from usage or navigation on its website

Automated Decision Making with legal or similar significant effect	processing which may lead to exclusion/discrimination
Systematic Monitoring	processing to observe, monitor and control individuals e.g. CCTV
Sensitive data or data of a highly personal nature	Article 9 (Special Category) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation May also include Criminal convictions, intrusive personal information, financial data
Large scale processing	No definition however the follow may help assess: 1. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; 2. the volume of data and/or the range of different data items being processed; 3. the duration, or permanence, of the data processing activity; 4. the geographical extent of the processing activity.
Matching or combining data sets	2 different data sets which are processed for different purposes being combined and used for reasons not reasonably expected
Data concerning vulnerable data subjects	E.g Learning Support
Innovative use or applying new technological or organisational solutions	Any introduction of new technologies or software.
Prevents data subjects from exercising a right or using a service or contract	Example, if the College sought consent to process data however was unable to meet the individual's Right to Object or withdraw consent.

The following template should be completed for all new processing activities to determine if it is appropriate for a DPIA to be carried out. It will allow the College to evidence why a DPIA has not been carried out if such a query is raised in the future.

DPIA Screening Form

This exercise should be completed for any new activity that requires the processing of personal data

Project/Contract Name:

Department/School:

1. PROJECT SUMMARY
Processing objective

2. STAKEHOLDERS
The main stakeholders for this project, in SERC, are:

3. BRIEF DESCRIPTION OF PERSONAL DATA INVOLVED
Categories, special category?

4. PRIVACY ASSESSMENT			
Use this checklist to assess the project for privacy risks. The questions below will help you consider whether a DPIA is necessary.			
(i) Does the activity involve any of the following high risk processing?	**Yes**	**No**	**If yes, explain your response**
Systematic or extensive profiling, evaluation or scoring	☐	☐	
Large scale processing of sensitive data	☐	☐	
Systematic monitoring of individuals	☐	☐	

Use of new technology or novel use of existing technology (e.g. AI)	☐	☐	
Denial of individuals' access to a service	☐	☐	
Profiling of individuals on a large scale	☐	☐	
Processing of biometric data	☐	☐	
Processing of genetic data	☐	☐	
Processing of sensitive data or data of a highly personal nature	☐	☐	
Combining, comparing or matching data obtained from multiple sources	☐	☐	
Invisible processing	☐	☐	
Tracking geolocation or behaviour	☐	☐	
Targeting of children or other vulnerable individuals	☐	☐	
Risk of physical harm	☐	☐	
If you answer yes to any of the questions in section 4(i) above, it is likely that a DPIA will be automatically required. Consult with SERC Data Protection Officer for further advice.			
(ii) **Does the project involve any of the following?**	**Yes**	**No**	**If yes, explain your response**
Automated decision-making with a legal or similar significant effect.	☐	☐	
Processing of data on a large scale.	☐	☐	
A change to an existing policy, process or system that involves personal data (e.g. new legislation or policy that makes it compulsory to collect or disclose information).	☐	☐	
A change in location of a business area or branch (e.g. plans to centralise a service or an office move).	☐	☐	
A practice or activity that is listed on a risk register (e.g. activities listed on your business area's risk register or health and safety register).	☐	☐	

Collecting new information about an individual (e.g. gathering information about individuals' location).	☐	☐	
A new way of gathering personal information (e.g. collecting information online rather than on paper forms).	☐	☐	
A change in the way personal information is stored or secured (e.g. cloud storage).	☐	☐	
A change to how sensitive personal information is managed (e.g. moving health records to a new database).	☐	☐	
Transferring personal information offshore (e.g. using a cloud based application to store data).	☐	☐	
A decision to retain personal information for longer than previously kept (e.g. keeping information for 10 years when you previously only held it for 7).	☐	☐	
Using information classed as 'special category data' (e.g. information about an individual's health).	☐	☐	
Using personal data already held for a new purpose (e.g. to obtain customer profiles).	☐	☐	
Disclosing information to a third party (e.g. following a request from a law enforcement agency to provide information for a particular purpose).	☐	☐	
Sharing or matching personal information held by different organisations or in different datasets (e.g. combining data with other information held on systems or sharing information to enable organisations to provide services jointly).	☐	☐	
A change in policy that results in people having less access to information that you hold about them (for example, archiving documents after 6 months into a facility from	☐	☐	

which they cannot be easily retrieved).			
Establishing a new way of identifying individuals (for example, a unique identifier, a biometric, or online identity system).	☐	☐	
Introducing a new system for searching individuals' property, persons or premises (e.g. adopting a new policy of searching data on mobile phones that have been returned for upgrading).	☐	☐	
Surveillance, tracking or monitoring of movements, behaviour or communications (e.g. installing a new CCTV system or monitoring a member of staff's email account).	☐	☐	
Changes to premises impacting on private spaces where clients/staff may discuss personal data (e.g. changing the location of a reception desk where people may disclose personal details or relocating a branch where sensitive personal data is processed).	☐	☐	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them (e.g. a*dding a new medical condition to the requirements of a licence.*	☐	☐	
Other privacy intrusions such as body searches, or intrusion into physical space.	☐	☐	

Additional Comments/Notes

5. INITIAL RISK ASSESSMENT		
If you answered 'Yes' to any of the questions in section 4, use the table below to give a rating - either Low (L), Medium (M), or High (H) – to each of the aspects of the project set out in the first column. If you answered 'No' to all the questions in section 4, move on to section 6.		
Aspect of the Project	**Rating (L, M or H)**	
Level of personal data handling	L – Minimal personal information will be handled	☐
	M – A moderate amount of personal information (or information that could become personal information) will be handled	☐
	H – A significant amount of personal information (or information that could become personal information) will be handled	☐
Sensitivity of information	L – The information is not sensitive	☐
	M – The information may be considered to be, or may become, sensitive	☐
	H – The information is highly sensitive	☐
Significance of the changes	L – Only minor change to existing functions/activities	☐
	M – Substantial change to existing functions/activities; or a new initiative	☐
	H – Major overhaul of existing functions/activities; or a new initiative that's significantly different	☐
Interaction with third parties	L – No interaction with other agencies	☐
	M – Interaction with one or two other agencies	☐
	H – Extensive cross-agency (government) interaction or cross-sectional (non-government and government) interaction	☐

Public impact	L – Minimal impact on the organisation and individuals	☒
	M – Some impact on individuals is likely due to changes to the handling of personal information; or the changes may raise public concern	☐
	H – High impact on individuals and the wider public; concerns over aspects of project or negative media interest is likely.	☐

6. SUMMARY OF PRIVACY IMPACT	
The privacy impact for this project has been assessed as:	
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated.	☐
Medium* – Some personal information is involved, and several low to medium risks have been identified	☐
High* – Sensitive personal information is involved, and several medium to high risks have been identified	☐
Reduced risk – The project will lessen existing privacy risks	☐
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	☐
Briefly summarise reasons for the rating given	

* If you have assessed the privacy impact as medium or high, a DPIA must be carried out.

7. RECOMMENDATION	
A full data protection impact assessment **is** required	☐

A full data protection impact assessment **is not** required	☐
Reasons	

8. SIGN OFF	
Information Owner/Representative:	
Name: xxxxxx	Date:
Signed:	
Data Protection Officer:	
Name: xxxxxx	Date:
Signed:	

9.2 What information should the DPIA contain?

1. A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
2. An assessment of the necessity and proportionality of the processing in relation to the purpose.
3. An assessment of the risks to individuals.
4. The measures in place to address risk, including security and to demonstrate that you comply.
5. A DPIA can address more than one project.

9.3 Who should be involved?

The Head of Department/ or Manager, relevant staff and the Data Protection Officer should complete the DPIA.

A DPIA is invalid without the involvement and approval of the DPO.

9.4 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.

9.5 Consultation with the ICO

If the **D**PIA 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.

9.6 When does a DPIA 'close'?

A DPIA must remain active for the duration of the processing activity. If anything changes e.g. types of data, lawful basis, procedures, the DPIA must be reviewed to reflect these changes and consider the impact on the individuals concerned.

Data Protection Impact Assessment (DPIA)

Template

The Data Protection Officer (DPO) must be consulted at the earliest opportunity. The DPIA must be signed off by the data owner and the DPO before processing can commence. The envisaged processing must be looked at objectively, and adjustments made where risk is identified.

PROJECT:_____

1. Identify the need for a Data Protection Impact Assessment
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

2. Describe the processing
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor

in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

3. Consultation process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

4. Access necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

5. Identify and assess risks			
Describe the source and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm (Remote, possible or probable)**	**Severity of harm (Minimal, significant or severe)**	**Overall risk Low, medium or high)**

6. Identify measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk (Eliminated, reduced or accepted)**	**Residual risk (Low, medium or high)**	**Measure approved (Yes/No)**

7. Sign off and record outcomes		
Item	**Name/Date**	**Notes**
Measures approved by:		**Integrate actions back into project plan, with date and responsibility for completion**

Residual risks approved by:		**If accepting nay residual high risk, consult the ICO before going ahead.**
DPO advice provided		**DPO should advise on compliance, step 6 measures and whether processing can proceed.**
Summary of DPO advice:		
DPO advice accepted or over-ruled by:		**If over-ruled, you must explain reasons**
Comments:		
Consultation responses reviewed by:		**If your decision departs from individuals views, explain.**
Comments:		
This DPIA will be kept under review by:		**The DPO should also review ongoing compliance with DPIA**

10 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 which 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?

10.1 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

Data Sharing Agreement (DSA)

Template

1. Parties to the Agreement	
2. Introduction	
3. Purpose	
4. Legal Basis for Data Sharing	
5. Organisations Involved	
6. Data to be Shared	
7. How Information will be Shared	

8. Information Use
9. Requests for Information / Complaints
10. Responsibilities of Each Party
11. Security
12. Retention and Disposal
13. Training
14. Security Incidents or Data Breaches
15. Review/Termination of Data Sharing Agreement

16. Indemnity

17. Signatures

I have read, understood and agree to abide by the terms and conditions of this Agreement. All information received will only be used for the purpose defined and listed in the Agreement.

Signed on behalf of xxxxxx (Data Controller)

Name (block capitals):

Date:

Signed on behalf of xxxxxx (xxxxxxxxx)

Name (block capitals):

Date:

11 Direct Marketing (Marketing of SERC Products, Services and Values)

Staff who wish to market products and services offered by and the values of SERC should refer to this guidance which details the conditions which **must** be met before communications are issued. Individuals have rights in relation to electronic communications including:

- Marketing emails, calls, texts and faxes
- Cookies

*****Please note, 'Direct Marketing' communications do not constitute standard communications such as emails detailing new College procedures, class cancellations/postponements, course progression to current students.

Examples of Direct Marketing would include the promotion of courses and events. You may however market courses to an individual if it is similar to a programme which the individual has previously attended. Please refer to the checklist for guidance on this.

The General Data Protection Regulations (UK GDPR) provides individuals with rights including the Right to Object which includes the objection to Direct Marketing. There will never be an overarching reason when this Right to object to Direct Marketing can be overruled.

Direct Marketing is regulated by the Privacy and Electronic Communications Regulations 2003 (PECR). These Regulations sit alongside and the Data Protection Act (2018), protecting individuals rights to privacy.

11.1 Definitions

11.1.1 Subscribers

For the purposes of marketing communications, the customer is referred to as a 'subscriber'. There are 2 types of subscriber:

Individual Subscriber: The contact details are the personal details of an individual e.g. xxxx@yahoo.com

Corporate Subscriber: The contact details are for business purposes e.g. xxxx@businessname.ac.uk

11.1.2 Solicited Material v Unsolicited Material

For the purposes of clarity, there are 2 types of Marketing.

Solicited: This is material which has been actively requested by the subscriber. PECR does not apply (although you must still say who you are, display your number when making calls, and provide a contact address).

Unsolicited: An unsolicited message is any message that has not been specifically requested. So even if the customer has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with PECR). But this is not the same as someone specifically contacting you to ask for particular information.
This does not make all unsolicited marketing unlawful. You can still send unsolicited marketing messages – as long as you comply with PECR.

11.2 Methods of communication

11.2.1 Email/SMS Communications

Staff must never send direct marketing materials via their Outlook account or mobile phones. Subscribers must be provided with the opportunity to 'unsubscribe' with each communication. Outlook and mobile phones do not provide this automated service.

11.2.2 Dotmailer

As an alternative to sending emails via Outlook, the following departments will issue email communications via the third-party provider 'Dotmailer' which has the default facility to offer 'unsubscribe'.

- Marketing
- Community Development
- Business Engagement

Dotmailer is for the purpose of communicating in bulk with subscribers. Should a person wish to opt out of future communications, their new preference is automatically updated in a suppression list and their details excluded from future correspondence.

11.2.3 Online Application Portal

The Online Application Portal allows staff to send communications to the subscribers via email and text.
When sending marketing communications via text/SMS or email to current students, the following departments will issue these via the 'Online Application Portal':

- School Support
- Customer Services
- Training Organisation

Any member of staff sending Marketing material to a current student can use this facility as it offers the mandatory 'unsubscribe' preferences. Please follow any on-screen instructions to flag your mail as 'Marketing'.

11.3 Privacy Suite

The Privacy Suite is available at privacy.serc.ac.uk and allows subscribers to manage their own marketing preferences. Preferences are automatically updated in Dotmailer and the Online Application Portal.

Should a subscriber contact the College and ask to be removed from Marketing communications, staff can direct the subscriber to the Privacy Suite at privacy.serc.ac.uk or staff can update their preferences subject to the customer providing the correct email address/mobile number (whichever method is receiving the communications).

Under no circumstances should staff accept any information changes from someone other than the account owner of the email address or mobile number.

11.4 Direct Marketing Checklist

Regulation	Individual Subscribers	Corporate Subscriber
(19) Automated Calls	Do not make unsolicited automated marketing telephone calls without **prior** consent.	Do not make unsolicited automated marketing telephone calls without **prior** consent.
(20) Faxes	Do not send unsolicited marketing faxes to individual subscribers without **prior** consent	Do not send unsolicited marketing faxes to numbers registered with the Fax Preference Service (FPS)
(21) Live Telephone Calls	Do not make unsolicited marketing telephone calls to subscribers who are either: Registered with the Telephone Preference Service (TPS) or Have previously asked the company not to call them	Do not make unsolicited marketing telephone calls to subscribers who are either: Registered with the Corporate Telephone Preference Service (CTPS) or Have previously asked the company not to call them
(22) Electronic Mail (emails, text messages)	Do not send unsolicited marketing material by electronic mail to individual subscribers without prior consent. Only exception to this rule is the 'soft opt in'. Only valid where a company can meet all 3 criteria: • The company have obtained the contact details for the recipient **in the course of a sale, or the negotiations for the sale, of a product or service to that recipient.** • The direct marketing material they are sending is only about **their own similar products and services.** • The recipient was given a simple means of opting out at the	No requirement for prior consent to send electronic mail marketing to corporate subscribers. However, the company must identify themselves and provide valid opt out facility in communications.

	time their details were initially collected and is given an **opt out** opportunity at the time of each subsequent communication	

12 Disclosures to Police

There may be occasions where staff will be approached by police personnel for information such as personal data, CCTV footage.

Staff should contact the Campus/Duty Manager in the first instance who will assess the validity of the request.

The Police should present the appropriate documentation to evidence their authority to make the request and the lawful basis for the request.

Depending on the nature and gravity of a request, there may be exceptions to the requirement of this documentation. The Campus/Duty Manager will assess the urgency of the request at the time.

13 Disposal of Records

Under the UK GDPR, data controllers (i.e., businesses using personal data,) should not retain personal data for any longer than necessary. Furthermore, the UK 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 UK 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

13.1 Transfer of Records to Public Record Office for Northern Ireland (PRONI)

(This guidance should be read alongside the FE Sector Retention and Disposal Schedule)
The FE Sector Retention and Disposal Schedule provides guidance to all staff on how to manage College records by providing timeframes for each record type and the 'Final Action'.
The Final Action will be one of the following, depending on the record:

1. Destroy
2. Permanent Retention by the College
3. Public Record Office Permanent Preservation
4. PRONI Appraisal
5. College Appraisal

Where the Final Action is 'Public Record Office Permanent Preservation', the College must arrange for the relevant records to be transferred to PRONI.

13.1.1 Identifying Records

All staff are aware of the requirement to carry out periodic appraisals of documents (once a year as a minimum). It is the responsibility of all managers to be aware of which records fall within their area of responsibility.

When staff are appraising documents, they must refer to the FE Sector Retention and Disposal Schedule to ensure the appropriate action is taken for each record type.
If the Schedule indicates their records have been identified for Public Record Office Permanent Preservation, the Head of Department/School should be notified, and the Data Protection Officer contacted immediately.

The DPO will contact the PRONI to arrange for the documents to be transferred.
The transfer of records from the College to PRONI is a legal process due to PRONI now becoming the lawful custodians of the documents.

In conjunction with the College, PRONI will issue a 'warrant' for the College to transfer records to PRONI detailing the nature of the records they are requesting.

The warrant will also contain a PR14 form which the Manager and DPO will review, complete and return to PRONI. This form will detail the College instructions as to whether the record should be a complete disclosure, partial disclosure, closed and the reasons why e.g., Public Interest Test, data protection considerations. The DPO will retain a copy of this record.

In advance of the transfer, Managers must arrange for all records within the scope identified on the Schedule are securely collated for collection. If the records are electronic, they must be password encrypted.

The DPO will liaise with PRONI to arrange the transfer of the records.

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.

14 Email Etiquette

Emails are now the most dominant forms of communication providing evidence of work activities, decisions, consultation between different departments/external agencies and are therefore discoverable.

With increased obligations towards transparency and access to information it is important for staff to be aware that all communications can be requested within the scope of Freedom of Information and Data Protection requests. Requests can be submitted by anyone including staff, students, parents, MLA's, councilors, legal representatives.

14.1 Always ✓

- Check the 'subject' field accurately reflects the content of your email - should be short and meaningful. This allows ease of retrieval at a later date.
- All records and communications, including emails must be written using appropriate language and grammar suitable for a public document.
- Consideration should be given to the choice of language used and tone to minimise the risk of the content being misinterpreted and thus causing unintentional distress. People's perceptions differ – caution will help avoid ambiguity.
- If your email is emotionally charged, wait before composing your reply. Review the sender's email again so that you are sure you are not reading anything into the email that simply isn't there.
- Be sure you are including all relevant details or information necessary to understand your request or point of view. Generalities can many times cause confusion and unnecessary back and forth.
- Comments about staff/students should be written with caution – remember you may be asked to justify it later….
- If factual information is of a negative nature e.g a student's failure to conduct him/herself appropriately in class, it is acceptable to record that but do so in a professional manner.
- Check the content of the email trail before selecting 'forward'. Is the recipient entitled to see previous contents.

14.2 Never X

- Do not 'bold' or 'underline' unnecessarily.
- Avoid inappropriate use of capitals and exclamation marks – it can be misinterpreted as shouting.
- Never write in anger – stop and reflect. Records cannot be edited/deleted subject to a request even if you think it may cause you embarrassment.
- Do not make unnecessary comments if not based on fact – you may be challenged and asked to validate your comments.
- Unnecessarily 'cc' people in as this creates excess copies of your communications for discovery.
- Do not make flippant, inflammatory or subjective comments - The focus of the communication may request a copy and rightly object if they are not happy with the context in which something has been written - is there an alternate tone which could convey the same information.

14.3 Note:

By issuing the above guidance, the College is not suppressing fair comment or justified opinion. This guidance is to always promote professionalism when recording such information and minimise the risk of distress to the individual(s) concerned and damage to College reputation.

15 Procedure for Personal Email Addresses

As a data controller, (the College) must ensure that any processing of personal information for which it is responsible complies with the Data Protection Act 2018 (DPA 2018). This includes using personal email addresses correctly to remove the potential for a security breach if these addresses are not handled securely, where appropriate. This procedure states the process for ensuring email addresses are used correctly.

15.1 Types of email address: personal, business or both?

An email address is personal data if an individual can be identified from it. Therefore, it is very important to think carefully before sharing such email addresses with others.

Some personal email addresses are private while others are professional / business related. For example:

- Joe@company.com is a personal email address which is business related, as it is assigned to a specific person at a company and gives enough information to identify a specific person at a company.
- Joe.Bloggs@serc.ac.uk is also a personal email address which is business related, as it is assigned to a specific person in the College and gives enough information for them to be identified.
- Info@serc.ac.uk is not a personal email address.
- Joe.Bloggs@hotmail.com is a private personal email address.

Other email addresses require a judgement to be made on whether they are personal because they do not include a name but may allow an individual to be identifiable, for example, jmck45@gmail.com. This judgement will depend on the circumstances of each case and best practice would be to err on the side of caution in cases of doubt.

15.2 To, Cc and Bcc Fields

When sending an email there are 3 available recipient fields: 'To', 'Cc' ('carbon copy), and 'Bcc' (blind carbon copy).

Using the 'To' and 'Cc' options means that each email address is shared with the other recipients. Using the "Bcc" option means that the recipient can only see their own email address.

15.3 Sharing Personal Email Addresses

The decision on which of the "To", "Cc" or "Bcc" fields be made in line with the College

It is College policy that student communications are only permitted through college email addresses or the Learner Management System. Staff must not use personal email addresses to contact students.

Personal email addresses can be shared if you have the individual's agreement to do so **(does not apply to student or applicant communications)** or if you are content that they would have a reasonable expectation of this and there is a business reason for doing so. For example:

- The personal email addresses of College staff can be shared both internally and externally in the 'To' or 'Cc' fields where this is necessary to conduct the College's official business.

This is because all staff will have a reasonable expectation of this type of sharing, and it forms part of the employment relationship.

- The personal email addresses of anyone else external to the College can also be shared both internally and externally using the 'To' or 'Cc' fields where this is necessary to conduct the College's official business and those concerned have a reasonable expectation of this or have agreed to it. An example of where this may be appropriate would be in the case of a working group where members of that group need to correspond with each other and be aware of who has been copied into correspondence.

It is helpful to ask yourself if you are justified in sharing personal email addresses by considering the following:

- Are the personal email addresses professional / business or private personal email addresses?
- Has the individual agreed to their personal email address being shared? What is their reasonable expectation? For example, have you advised the individual how their personal data will be used, through a privacy notice?
- Have you previously sent the personal email address via 'To' or 'Cc' in a group email for a very specific purpose? Have you ever received an objection from those individuals in relation to that purpose?
- How would you justify the use of the 'To' and 'Cc' fields if you are challenged?

If an email address does not identify any individuals, then you do not need to use the "Bcc" field. Likewise, if you are sending an email to only one recipient then you do not need to use the "Bcc" field.

15.4 Email Addresses shared in error

If you discover that an email has been sent with a private personal email address in the "To" or "Cc" field in error, **you should not attempt to recall the message** as this may exacerbate the breach. Another important factor is that most (if not all) recipients will see the recall request and it will again include all the recipients' email addresses, with the result that the data breach will be repeated.

Any data breaches should be reported to your line manager immediately and the data protection officer at informationrights@serc.ac.uk

15.5 Recommended Good Practice

The following points will support staff in in avoiding embarrassment, misunderstandings and give confidence that you can justify your emails in the event they are subject to disclosure.

16 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:

16.1. 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 generate unnecessary amounts of paper which increases the risk of potential loss of data or attaching 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.

16.2. Staff Areas

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

16.3. Forwarding Emails

- When you forward an email to others or copy a 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.

16.4. 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.

16.5. 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.

16.6. Discussions

- It is easy to forget when discussing business with Colleagues especial 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 can hold it in a more confidential space.

17 Legitimate Interest Assessment

The 6 main lawful basis for processing personal data are:

- Consent
- Contract
- Legal obligation
- Vital Interest
- Public Task
- Legitimate Interest.

Where the College is relying on **Legitimate Interest** to process personal data, a Legitimate Interest Assessment (LIA) must be completed prior to the commencement of the processing activity.

The LIA is a 'business case' to justify your need to process the activity in question and evidence that the 3 main privacy tests have been properly considered:

17.1 Purpose Test

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice? Are there any other ethical issues with the processing?

17.2 Necessity Test:

- Will this processing help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

17.3 Balance Test:

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

The DPO should be contacted for guidance at the earliest opportunity and must countersign the assessment along with the data owner.

Please note, the College is not permitted to rely on Legitimate Interest if the processing form part of our Public Task.

Failure to complete an LIA will deem your processing invalid and without a Lawful Basis.

Legitimate Interest Assessment (LIA)

Template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

PROJECT:_____

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose Test ***You need to assess whether there is a legitimate interest behind the processing.***
• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity Test **You need to assess whether the processing is necessary for the purpose you have identified.**
• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing Test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

Reasonable Expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?

Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?

• Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes/No

Making the decision	
This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.	
Can you rely on legitimate interests for this processing?	Yes/No

Signatures

Data Owner:

Date:

Data Protection Officer:

Date:

What's next?

18 Overseas Data Sharing

Transfers of personal data outside of the UK, to third countries or international organisations is restricted under the UK GDPR. This is to ensure that the level of protection to individuals provided by the UK GDPR is not undermined.

18.1 Overview

Chapter V of the UK GDPR states the transfer of personal data to a third country or to an internal organisation can take place only if the conditions laid down under Chapter V are complied with.

As the UK left the EU on the 31st December 2020, a transition period of six months was agreed as part of the Trade and Cooperation Agreement. In June 2021 the EU Commission announced the UK's adequacy decision had been approved. This will allow for the continued free-flow of personal data between the UK and EU for an initial period of four years. The UK has approved the EU's adequacy on a reciprocal basis.

18.2 Safeguards

Personal data may be transferred outside of the UK 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 in a corporate group)
- standard data protection clauses in the form of template transfer clauses adopted by the Information Commissioner's Office
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Information Commissioner
- compliance with an approved code of conduct approved by the Information Commissioner.
- certification under an approved certification mechanism as provided for in the UK GDPR;
- contractual clauses agreed authorised by the Information Commissioner.
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the Information Commissioner.

18.3 UK Adequacy Decisions

The UK has adequacy decisions for a number of countries that have been adopted from the EU Commission's. This allows for the free-flow of personal data without the need of additional safeguards. The following countries and territories currently have adequacy decisions:

- European Economic Area (EEA)
    - Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden
    - Iceland, Norway, and Liechtenstein
- Gibraltar
- EU Commission full finding of adequacy countries
    - Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay
- EU Commission partial findings of adequacy
    - Japan (Private Sector organisations only)

- Canada (Data subject to PIPEDA only)

The transfer of personal data between the UK and the USA requires additional protections and safeguards. The European Court of Justice (CJEU) deemed the EU-US Privacy Shield as invalid. At present the UK does not have an approved adequacy decision for USA.

18.4 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 UK GDPR.

Authorisations of transfers made by the UK government or Information Commissioner regarding adequate safeguards made under the UK GDPR will remain valid/remain in force until amended, replaced, or repealed.

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

The UK GDPR provides derogations from the general prohibition on transfers of personal data outside the UK 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 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.

18.6 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 UK GDPR provides that personal data may still be transferred outside the UK.
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 Information Commissioner of the transfer and provide additional information to individuals

19 Parent/Next of Kin Contact

The College welcomes and encourages contact with parents/next of kin however we must always be satisfied that this contact is lawful. The main condition which would support this contact is:

19.1. Consent:

The on-line application portal should be checked to confirm whether or not a student consents to their parent being contacted.

19.2. Exceptions:

Where there is concern regarding the life, health or well-being of a student, staff do not need consent to discuss concerns with an appropriate individual however, disclosures must be on a ‘need to know’’ basis. Staff should take into consideration already known information when assessing if the parent/next of kin is the appropriate person to contact.

20 Photography/Videography

An individual's name, video/audio/photo/testimonial can be considered as personal data and has been viewed legally as special category data.

Staff wishing to take photos/videos must refer to the *'Communications and Marketing SOP'* which details conditions which must be met with each processing activity.

21 Privacy Notices

21.1 What is a Privacy Notice?

The first Principle of UK 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.

21.2 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

21.3 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

21.4 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.

21.5 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	✓	✓

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
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		✓
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

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
		latest, when the first communication takes place; or • If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

22 Removing Personal Identifiers

22.1 Anonymisation

Anonymisation is a valuable tool that allows data to be shared, whilst preserving privacy. The process of anonymising data requires that identifiers be 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.

22.2 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, e.g., 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 – e.g., reference numbers – but not the 'key' needed to link these to 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 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.

22.3 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.

22.4 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 (e.g., 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 many 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 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 analyses social trends on a regional basis, for example.

22.5 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 e.g., 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.

23 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.