NATIONAL COLLEGE OF IRELAND DATA PROTECTION POLICY

January, 2018

Document Information

Prepared By:	Natalie Murphy	**Document Version No:**	0.4
Title:	Data Protection Policy	**Document Version Date:**	23/05/2018
Reviewed By:	National College of Ireland	**Review Date:**	

Distribution List

To	Action	Due Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description
0.1	22/01/2018	Natalie Murphy	Initial Document Created
0.2	21/02/2018	Natalie Murphy	First round of feedback included
0.3	16/03/2018	Natalie Murphy	Feedback from HR department
0.4	23/05/2018	Natalie Murphy	Updated in line with suggestions from NCI legal counsel
0.5	08/09/2020	Niamh Scannell	Corrected error in handling rules in online version
0.6	15/03/2022	Niamh Scannell	Updated links in section 1.4

***Enter document details in the in the tables above and make sure to update as changes are made**

CONTENTS

1 INTRODUCTION

In line with data protection requirements and good practice, National College of Ireland ('NCI') wish to put in place, and be able to demonstrate, appropriate and effective management of personal data throughout the Organisation.

NCI wishes to demonstrate commitment and compliance with the current Data Protection Acts and the General Data Protection Regulation (GDPR). Fundamental to the GDPR are the principles of accountability and transparency. This means that Controllers and Processors are both responsible and, accountable for the protection of personal data, and must be able to demonstrate how they maintain compliance with data protection requirements.

The implementation of an approved Data Protection Policy goes towards demonstrating NCI's commitment to the protection of personal data, and provides a basis for maintaining and improving compliance with data protection requirements and good practice.

1.1 PURPOSE OF THIS DOCUMENT

NCI collects, processes, and stores significant volumes of personal data and sensitive personal data (special category data) on an ongoing basis. NCI are committed to complying with data protection legislation and good practice.

The purpose of this document is to provide a statement of intentions and directions of NCI for managing compliance with data protection requirements which is formally approved by senior management. The aim of this policy is to ensure that any individual who handles personal data, whether they are a member of staff or a contractor, is fully aware of the requirements and act in accordance with data protection procedures.

The objectives of the data protection policy are to:

1. Enable NCI to meet its own requirements for the management of personal data.
2. Ensure NCI meets applicable statutory, regulatory, contractual and/or professional duties.
3. Protect the interests of individuals and other key stakeholders.
4. Support organisational objectives and obligations.
5. Impose controls in line with NCI acceptable level of risk.

This document also highlights key data protection procedures within NCI.

1.2 SCOPE AND CONSTRAINTS

This policy applies to all personal data processed by NCI, regardless of the media on which the personal data is stored (paper-based, electronic, CCTV or otherwise).

This policy applies to:

- any person who is employed by NCI or is engaged by NCI, whether on a paid or voluntary basis, including contractor and sub-contractors, and who process personal data in the course of their employment or engagement.

Failure of any staff member or agent to comply with this policy may lead to disciplinary action being taken in accordance with NCI's disciplinary procedures. Failure of a third party

contractor/subcontractor to comply with this policy may lead to termination of the contract and/or legal action.

1.3 Policy Review, Approval, and Continuous Improvement

In line with best practice, this policy has been approved by senior management, along with a commitment of continual improvement. This document will be reviewed at least annually by senior management and the NCI Data Protection Officer to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, legal developments, legislative obligations, and information commissioner guidance.

1.4 References

1. General Data Protection Regulation (ref: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679)
2. Data Protection Act 2018 (ref: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html)
3. E-Privacy Directive (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)
4. S.I No. 336/2011 – European Communities (Electronic Communications, Networks, and Services) (Privacy and Electronic Communications) Regulations 2011 (ref: http://www.irishstatutebook.ie/eli/2011/si/336/)
5. Guidelines 07/2020 on the concepts of "controller" and "processor"in the GDPR (ref: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
6. Guidelines, recommendations, and best practice issued by the European Data Protection Board (ref: Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board (europa.eu)

This document forms part of the NCI Personal Data Management System, and should be read in conjunction with the other documents within the management system:

- NCI Data Retention Policy (Document Reference: NCI-PDMS-03)
- NCI Privacy Notice(s) (Document Reference: NCI-PDMS-04)
- NCI Data Breach Incident Procedure (Document reference: NCI-PDMS-05)

1.5 Definitions

The following key GDPR terms and definitions are provided here for ease of use. For a complete list of definitions refer directly to the regulation (ref: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1465452422595&uri=CELEX:32016R0679).

1. '**Anonymisation'** is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

2. **'Personal Data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Recital 26 also clarifies anonymous information "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes*".

3. '**Special Categories of Personal Data'** refers to the processing of 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.

   NCI will avoid all processing of special categories of personal data where possible. It is understood that certain business activities within NCI require the processing of special categories of data (e.g. processing of data concerning health and disability). The general processing of special categories is prohibited in NCI, and in the rare instance it is required, Head of Departments must ensure all processing is defined in the data inventory, along with an appropriate legal basis (reference 1, Art 6), and derogation (reference 1, Art 9) for processing of such special categories recorded within the data inventory.

4. **'Data controller'** means the natural or legal person, public authority, agency or another body which, **alone or jointly with others**, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

   In certain instances, NCI alone determines the purpose and means of processing, and in other instances, NCI might jointly determine the purpose and means of processing with a third party. In both circumstances, NCI would be considered a controller of this information. Section 8 of this policy provides further information on the responsibilities of controllers, processors, and third parties.

5. '**Data subject'** any living individual who is the subject of personal data held by an organisation. Data subjects within NCI may include members of the public, students (current, past, and prospective), employees (current, past, and prospective), suppliers (e.g. sole traders or staff acting on behalf of the supplier), and other individuals such as external third parties, CPD members, and any other individual NCI might communicate with.

6. **'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

7. **'Processor'** means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

8. **'Third Party'** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons, who, under the direct authority of the controller or processor, are authorised to process personal data

9. **'Profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person. This can include analysing or predicting aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

10. '**Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

    Examples of pseudonymisation within NCI may include the use of student IDs instead of student names for access authorisation. Where anonymisation cannot be used, the next best of pseudonymisation should be used.

11. **'Recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

2 ROLES AND RESPONSIBILITIES

All NCI staff and contractors are responsible for ensuring compliance with NCI's data protection requirements and obligations. It is the responsibility of all staff to ensure:

1. They familiarise themselves with this policy and handle personal data in accordance with this policy, the data protection principles, and data handling rules.
2. They complete the mandatory data protection training provided. Data protection training is mandatory for all NCI employees. Annually, all NCI staff will have to complete this training and a record maintained for audit purposes.
3. Queries in relation to personal data are promptly and courteously dealt with. When an employee receives an enquiry about the handling of personal data, they must know what to do, and/or where to refer it.

To ensure all users are aware of their responsibilities as users of NCI systems, the following sections include additional requirements based on key data protection roles within NCI.

While all staff and agents of NCI have a responsibility to ensure data protection compliance, the following sections include additional requirements for key, specific data protection roles within NCI.

2.1 Governing Body and Senior Management

The Governing Body and senior management are responsible for approving and reviewing this policy, and for mandating the allocation of appropriate resources to ensure its successful implementation. Each member of the Board is responsible for ensuring compliance with the Data Protection Acts and GDPR in their respective areas of responsibility.

2.2 Data Protection Officer

In line with the requirements of the GDPR and Data Protection Acts, NCI has appointed a Data Protection Officer. The individual performing the role of DPO must be suitably trained, independent, and of sufficient seniority to perform the tasks required. The role may be performed as a team function provided a single individual is the lead person "in-charge" and roles within the Data Protection Officer team are clearly defined.

Within NCI, our Data Protection Officer and the team may be contacted at:

Data Protection Officer Contact Details	
Name:	Niamh Scannell
Address:	Data Protection Officer IFSC Mayor Street North Dock Dublin 1 D01 Y300
Email:	dpo@ncirl.ie
Telephone:	(+353 1) 4498 523 or (01) 4498 523

The responsibility of the Data Protection Officer function within NCI is to:

1. Respond to individuals (data subjects) whose data is processed on all issues related to the processing of their data and the exercise of their data protection rights.
2. Cooperate with the Supervisory Authority, and act as the Organisation's contact point for the Supervisory Authority on all issues related to the processing of Personal data in NCI.
3. Inform and advise NCI and its employees of their obligations pursuant to privacy regulations.
4. Monitor compliance with the data privacy obligations in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations and the related audits.
5. To provide advice and assistance regarding the requirement to perform Data Protection Impact Assessments, and monitor their performance.
6. Arrange at least annual data protection training sessions.
7. Maintain a log of all data breaches and communication of breaches to all relevant parties when required to do so (Supervisory Authority, Controllers, and Data Subjects). Please refer to Section 6 for more details.

To allow for the effective performance of the Data Protection Officer's tasks, NCI will ensure:

1. The Data Protection Officer will be suitably trained and have expert knowledge of Data Protection Law.
2. NCI will support the Data Protection Officer in performing the tasks above by providing resources necessary to carry out those tasks. The key to this is to provide sufficient time, finance, and staff where appropriate to fulfil the Data Protection Officer duties.
3. No tasks and duties result in a conflict of interests for the Data Protection Officer.
4. That the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data, and will be in a position to perform their duties and tasks in an independent manner. Specifically:

    a. The Data Protection Officer will report directly to the NCI Board.
    b. The involvement of the Data Protection Officer will be sought where decisions with data protection implications are taken. All relevant information must be passed on to the Data Protection Officer in a timely manner in order to allow him or her to provide adequate advice.
    c. The Data Protection Officer will participate regularly in meetings with senior and middle management.
    d. The opinion of the Data Protection Officer will always be given due weight.
    e. The Data Protection Officer must be consulted without delay in the event of a data breach or other data protection incident occurring.

2.3 Human Resources

NCI human resources personnel have a key role in the management and protection of personal data which includes responsibility for:

1. Ensuring all new members of staff are made aware of this policy document at induction stage and that it is referenced in staff terms and conditions, contracts, and role descriptions.
2. Ensuring new starters and temporary staff who require training complete the first available data protection training course after their start date.
3. Handling all employee-related personal data in accordance with this policy, the data protection principles, and data handling rules.

2.4 Head of Functions and Departments, Business Owners, Line Managers

Line Managers and Heads of Functions or Departments have a key role in the management and protection of personal data which includes responsibility for:

1. Ensuring all processing within their department is in compliance with the NCI Data Protection Policy and privacy best practice. Specifically, maintaining the data inventory of all information processed by their department, and for ensuring that staff in their area are aware of the policy, and the general obligations and requirements of data protection.
2. Ensuring their reporting staff complete the mandatory data protection training.
3. Ensuring sufficient resources are available to support the effective implementation of this policy.
4. Ensuring appropriate technical and organisational security measures, including anonymisation for statistical and research purposes, are in place in areas for which they are responsible. Specifically, security risk assessments will be undertaken to check that the personal data is sufficiently protected in line with security policy. Security risk assessments will be commissioned regularly and evidence retained for audit purposes. To deal with appropriate technical and organisational security measures, the Line Manager/Head of Function may delegate the security tasks, in full or partially, to another NCI representative. This delegation does not exempt the Line Manager/Head of Function from their

responsibility and they must make sure that the delegated jobs have been carried out correctly.

5. Ensuring data privacy risks are appropriately managed within their function. Specifically, to ensure the handling of personal data is regularly assessed and evaluated. Under the GDPR, there are a number of changes which will affect both in-house changes and contracts for new projects. It is therefore important that if any new projects are being considered then data protection needs to be built in at the beginning (Privacy by Design and Default), and contracts will need to reflect the necessary changes.
6. Ensuring that where processing "is likely to result in a high risk to the rights and freedoms of natural persons" and/or "processing on a large scale of special categories of data", a Data Protection Impact Assessment is formally carried out in relation to each new project or proposal (see section 5 for more details on Data Protection Impact Assessment). The NCI Data Protection Officer must be consulted at each stage of the DPIA process in line with section 5.3 of this document.
7. Ensuring regular consultation with the Data Protection Officer, and facilitating the DPO in performing their compliance audits.

2.5 Technical Solutions Architects / Technical Design Leads / Project Managers

Members of staff and other third parties involved in the planning, design, build, and change of technical solutions have a key role in the protection of personal data which includes:

1. Ensuring the protection of personal data is considered for all changes and managed projects within NCI.
2. Where changes and projects do not include the collection and processing of personal data, this must still be documented and signed off by the Project Manager, and retained as evidence for audit purposes.
3. Implementing the principles of data protection by design and data protection by default, and retaining evidence of this for audit purpose as part of the Project Management Lifecycle (see Section 5 for more details).

3 How NCI complies with the Data Protection Principles

NCI is committed to ensuring all personal data is processed in line with the data protection principles and good practices. This includes:

3.1 "Lawfulness, Fairness and Transparency"

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

NCI is committed to ensuring the lawful, fair, and transparent collection of data. Our data inventory records all information processed, including the lawful basis of such processing. In addition, our privacy notice provides all necessary information to Data Subjects about the processing of their data. The information is given in a concise, transparent, intelligible, and easily accessible form, and includes the purposes of processing, the period of processing, their rights, and the lawful basis for the processing. These privacy notices must be provided to Data Subjects **prior to** collecting personal data regardless of the collection method (phone, CCTV, forms, interview, website etc.).

3.1.1 Where the lawful basis is "consent"

Where the lawful basis of processing is based on consent, NCI shall incorporate procedures for the obtaining and withdrawal of consent. Where consent is withdrawn, processing based on consent must cease. Specifically, where other departmental requirements or legislation require explicit consent (e.g. for marketing), the departments shall contain procedures for collecting this consent. The department must also monitor all requests for removal or withdrawals of consent, maintain a register of all such requests, and ensure that all removals are completed without undue delay.

Where processing on the lawful basis of consent, and the processing relates to a child (reference 2 – this is 16 years of age), the department must ensure they have obtained and recorded consent provided by the holder of parental responsibility for the child.

Refer to the NCI Data Protection Officer for further guidance, clarification, and consultation in relation to the lawfulness of processing, and conditions for consent.

3.2 "PURPOSE LIMITATION"

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

NCI is committed to only collect and process information for an explicit purpose. All information processed, along with the business purpose, is detailed within the data inventory which will be reviewed and updated at least annually, or when any significant changes occur to the data processed, where it is processed, or with whom it is shared.

Personal data will only be processed for the defined purpose. All requests for changes to the use of personal data must be compatible with the original purpose for processing. If additional purposes are required, consent may be required to be sought from the data subject for this change of purpose.

3.3 "DATA MINIMISATION"

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

NCI is committed to only collect and process appropriate information to the extent needed to fulfil the operational and service needs, and to comply with all applicable statutory, regulatory, contractual and/or professional duties. Data will be minimised, and the minimisation shall be enforced through Data Protection Impact Assessments (DPIAs), and Data Protection by Design and Default procedures within the change management/project management teams.

3.4 "ACCURACY"

Personal data shall be 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.

NCI is committed to taking all reasonable efforts to ensure the accuracy of the personal data. This will be planned for, and enforced, through DPIAs, and Data Protection by Design and Default procedures within our change management/project management teams.

3.5 "STORAGE LIMITATION"

Personal data shall be 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.

NCI have documented the required data retention periods along with justification and action to be taken when the retention period expires. The Data Retention Policy outlines the retention period for all personal data across NCI, and what will occur when the retention period expires. It applies to all personal data, regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise). This policy helps ensure that NCI is maintaining the personal data for an appropriate length of time, based on legal and business requirements and in line with the data protection 'storage limitation' principle. All staff and contractors are responsible for ensuring this policy is adhered to.

3.6 INTEGRITY AND CONFIDENTIALITY

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

NCI is committed to protect and not disclose personal data, either within or outside of NCI, to any unauthorised recipient. All staff and contractors are responsible for protecting personal data against accidental loss, destruction or damage, regardless of the media on which it is stored (paper-based, electronic, CCTV or otherwise).

4 INDIVIDUAL RIGHTS

All data subjects have a wide array of rights in relation to the personal data which NCI process on their behalf. The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist.

4.1 COMMON PROCEDURES TO EXERCISE INDIVIDUAL RIGHTS

Any queries regarding data protection, or any requests for personal data, whether from the person themselves or from a third party, must be referred to the Data Protection Officer. Any person wishing to exercise this right must apply in writing (or email) to the DPO.

The procedure is as follows:

1. All data access requests directed to NCI must be in writing (or email), to the DPO. On receipt of a query or access request by telephone, please ask the caller to put their request in writing (or email), and to address it to the NCI Data Protection Officer.

2. The DPO will check the validity of the access request. The GDPR does not introduce an exemption for requests that relate to large amounts of data, however, all efforts will be made to try to narrow the search to provide the data subject with relevant and concise information and avoid a disproportionate effort. Where the request is considered excessive, unfounded, or information which the data subject already holds, consideration will be given as to the validity of the request.

3. The request must include sufficient identification and details for the DPO to satisfy themselves that sufficient material has been supplied to definitively identify the individual. If the DPO can demonstrate they are not in a position to identify the data subject, additional information will be requested as necessary to confirm the identity of the data subject and the request will not be enacted upon until such identification is provided to the DPO. Personal data should never be provided to a data subject that has not been identified, nor should personal data be provided to the parent or legal guardian of a data subject where that subject is 16 years or older (reference 2).

4.2 Right to Access

Data subjects (including employees, students, other individuals and members of the general public that may have availed of NCIs services, or received communications or information from NCI) have the right to access personal data held about them (this includes factual information, expression of opinion, and the intentions of NCI in relation to them, irrespective of when the information was recorded).

1. Where the access request is relevant to a number of departments, the DPO will contact the relevant departments and request them, in writing, to conduct a search of all data held by them. Such searches will be conducted in accordance with guidance provided by the DPO, and all steps taken to locate and collate data will be noted and documented.

2. Each department must redact all information not relevant or not in scope for release. Where the department is unsure of what is relevant they must consult with the DPO. However, the responsibility for redacting irrelevant information remains with each department.

3. Once any required review and redaction are completed, the personal data that is recommended for disclosure/deletion will be forwarded to the DPO for consideration. Department responses must also include an analysis of the relevant exemptions being relied upon, a description of the purpose of processing, to whom the data may have been disclosed, and the source of the data.

4. If personal data relating to other parties (other than the requesting data subject) is involved, the personal data of the other parties must not be disclosed without their consent. Alternatively, the other party personal data may be anonymised so as not to reveal their identity. If an opinion of other parties (other than the requesting data subject) is involved, their opinion may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.

5. A final decision on disclosure/deletion of the requested information will be taken by the DPO, in conjunction with the head of the relevant department(s) and legal advice where required.

4.2.1 CCTV Footage

CCTV footage is personal data within the meaning of the Data Protection Acts. Any disclosure of CCTV footage must follow the same procedure as stated in steps 1-5 stated above, and be approved by the DPO. The following provides the *Irish Data Protection Commission's* position with regard to access to CCTV footage made under Subject Access Requests (reference DPC Annual Report Case Study 13 of 2013. This is available in the "pre-GDPR" section of their website):

1. *Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage.*

2. *When making an access request for CCTV footage, the requester should provide the data controller with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the approximate time and the specific date(s) on which their image was recorded. For example, it would not suffice for a requester to make a very general request saying that they want a copy of all CCTV footage held on them. Instead, it is necessary to specify that they are seeking a copy of all CCTV footage in relation to them which was recorded on a specific date between certain hours at a named location. Obviously, if the recording no longer exists on the date on which the data controller receives the access request, it will not be possible to get access to a copy. Requesters should be aware that CCTV footage is usually deleted within one month of being recorded.*

3. *For the data controller's part, the obligation in responding to the access request is to provide a copy of the requester's personal data. This normally involves providing a copy of the footage in video format. In circumstances where the footage is technically incapable of being copied to another device, or where the supply of a copy in video format is impracticable, it is acceptable to provide stills as an alternative. Where stills are supplied, it would be necessary to supply a still for every second of the recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.*

4. *Where images of parties other than the requesting data subject appear on the CCTV footage, the onus lies on the data controller to pixilate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requester. Alternatively, the data controller may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.*

5. *Where a data controller chooses to use technology to process personal data, such as a CCTV system to capture and record images of living individuals, they are obliged to shoulder the data protection obligations which the law places on them for such data processing. In the matter of access requests for CCTV footage, data controllers are obliged to comply fully with such requests. Claims by a data controller that they are unable to produce copies of footage or that stills cannot be produced from the footage are unacceptable excuses in the context of dealing with an access request. In short, where a data controller uses a CCTV system to process personal data, it takes on and is obliged to comply with all associated data protection obligations.*

The following provides the *UK Information Commissioners Office* with regard to access to CCTV Footage made under Subject Access Requests Ref: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf (please copy and paste this link into your browser for access)

When disclosing surveillance images of individuals, particularly when responding to subject access requests, you need to consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration should be given to the nature and context of the footage.

Example: If footage from a camera that covers the entrance to a drug rehabilitation centre is held, then consider obscuring the images of people entering and leaving it as this could be considered

sensitive personal data. This may involve an unfair intrusion into the privacy of the individuals whose information is captured and may cause unwarranted harm or distress. On the other hand, footage of individual's entering and exiting a bookshop is far less likely to require obscuring.

Following the above, a case-by-case assessment is required as to the context of the CCTV. If unsure, please refer to DPO.

4.3 Right to Rectification

Data subjects (including employees, students, other individuals and members of the general public that may have availed of NCI's services, or received communications or information from NCI) have the right to the rectification of any inaccurate personal data concerning him or her that is held by NCI. This applies if data is inaccurate or misleading to a matter of fact. This is not an absolute right, and restrictions apply. For example, it does not apply to witness statements or opinions of others such as assessors, etc. Refer the data subject to the DPO for all requests under the "Right to Rectification".

In the case of backups, the right to rectification may not be practical or possible, and may therefore be exempt. This would depend on the backup types, and the DPO should be consulted if there is any uncertainty.

4.4 Right to Erasure

Data subjects have the right to obtain from the controller the erasure of personal data concerning him or her where there is no longer a legal ground for processing of the information. This is not an absolute right, and restrictions apply. Refer the data subject to the DPO for all requests under the "Right to Erasure".

In the case of backups, the right to erasure may not be practical or possible, and may therefore be exempt. This would depend on the backup types, and the DPO should be consulted if there is any uncertainty.

4.5 Restrictions

There are restrictions, and in certain circumstances, it may be prudent for NCI not to adhere to certain individual rights. The Data Protection Officer will consider each request on a case by case basis and it is likely that such restrictions would not apply to the complete data set and more likely to a restricted and very specific set of personal data. For example, NCI may not be permitted to apply a blanket exemption to the right of access to an entire set of a student's data because some elements may be considered privileged, such as an opinion given in confidence regarding the student.

If NCI wishes to withhold certain subject rights, this must be referred to the DPO, who may seek legal counsel. Restrictions on exercise of data subject rights are laid out in the Data Protection Act (reference 2), and shall be considered carefully when performing data subject access requests.

It should be noted that the existence of proceedings between a data subject and the data controller, for any reason, does not preclude the data subject making a data subject access request under the Act, nor does it justify the data controller in refusing the request. For example, if a data subject access request is refused, a response clarification as to which exemption is being applied, including the specific restriction, must be cited.

5 INFORMATION AND CYBER SECURITY

The GDPR requires NCI to implement technical and organisational measures to ensure an appropriate level of security. NCI must take into account the current state and availability of security technologies, the costs of implementation, the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. NCI must also ensure their processors also implement appropriate measures. Some examples of appropriate measures as mentioned in the Regulation are:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

NCI fulfil these obligations by a number of means, specifically:

1. Deployment of Data Protection by Design and by Default within our Project Management Lifecycle for all new systems/changes to processing (reference Section 5.1 for further details).
2. Regular risk assessments/testing to assess and evaluate the effectiveness of technical and organisational measures on existing processing (reference Section 5.2 for further details).
3. Formalised Data Protection Impact Assessments (DPIAs) where processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" and/or "*processing on a large scale of special categories of data*" (reference Section 5.3 for further details).

Records of all of the above activities will be forwarded to the NCI Data Protection Officer and retained for audit purposes.

5.1 DATA PROTECTION BY DESIGN AND DEFAULT

The GDPR requires:

1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected,*

the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

As part of the implementation of Data Protection by Design and Data Protection by Default principles, a data protection and security design review will be performed during the development stage, and as part of the project management of all projects. The following is a minimum checklist for the areas that will be examined as part of this review, and records of the examination of each area must be maintained for audit purposes:

1. Has the Data Inventory been updated with any new forms of processing including data categories processed, where it is processed, and with whom it is shared?

2. Has a valid lawful basis for this processing been defined within the Data Inventory?

3. Do any new forms of processing include a relevant data privacy notice with all required information as defined in the NCI Data Privacy Notice(s) policy (reference NCI-PDMS-04)?

4. Is the information collected for a specifically defined purpose?

5. Is only the required information collected, or is information collected which may be deemed excessive (i.e. is the personal data that is collected minimised)?

6. How is the personal data kept reasonably accurate and up-to-date?

7. How long is the personal data retained for, and does the retention period and destruction method comply with the NCI Data Retention Policy (reference NCI-PDMS-03)?

8. Is it necessary for NCI to be able to identify the individuals whose data is being processed, or could anonymisation be used?

9. Could pseudonymisation be enforced to protect the personal data, for example, could individuals making enquiries regarding courses be restricted to a reference number until such time as they submit an application?

10. Can the personal data be encrypted at rest and/or in transit, and if not, are other security measures in place to adequately address the risks associated with the processing activity?

11. How is the information protected against unlawful or accidental loss, destruction or damage?

12. How does the new form of processing allow for the implementation of individual rights, including the right to access, rectification, and erasure?

13. Is all processing within the EEA?

14. Has a technical penetration test or risk assessment been performed and remediation actions were taken?

15. Are appropriate access controls in place? Specifically:

a. Is physical or remote access needed to the office in order to access the personal data?

b. Is user access restricted on a need-to-know basis?

c. Is all user access audited and do is there an audit trail of all user access?

d. Is there a formal process for joiners/movers/leavers to facilitate user access management?

e. Are user access reviews performed which are signed-off by relevant business owners and recorded for audit purposes?

16. Are other relevant and appropriate technical and organisational security measures applied? Specifically:

    a. Is a formalised patching policy applied and maintained?

    b. Are reliable and recent backups in place, and are these tested regularly?

    c. Are all backups encrypted?

    d. Are appropriate perimeter security controls applied?

    e. Is appropriate anti-malware deployed?

17. Can personal data which is shared externally for reporting purposes, or retained for analytics/statistics, be anonymised?

5.2 Regular Risk Assessment

The GDPR Requires:

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

It is the responsibility of the Head of the Department to ensure appropriate technical and organisational security measures are in place in areas for which they are responsible. Specifically, regular security risk assessments must be commissioned to check that the personal data is sufficiently protected based on the level of risk. Security risk assessments will be conducted regularly, and a record maintained for audit purposes with the output from each area examined. At a minimum, the risk assessment must evaluate and record the technical and organisational measures identified in the previous section (Section 5.1). Heads of Department may commission other NCI resources to assist with risk assessments.

NCI will ensure that any risks to the privacy of data are assessed, and that measures that are implemented are appropriate to the risks of the processing on the systems used. To facilitate this, each data category name, data store, and recipient/s (or third parties) are assigned a risk level based on a defined set of criteria for each department's Personal Data Inventory.

5.3 Data Protection Impact Assessment (DPIA)

The GDPR requires that a formalised Data Protection Impact Assessment (DPIA) is performed where processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" and/or "*processing on a large scale of special categories of data*".

A data protection impact assessment will be carried out by NCI prior to the processing of the personal data, paying particular attention to the likelihood and severity of the risk, taking into account the:

1. Nature
2. Scope
3. Context and purposes of the processing
4. The sources of the risk

At a minimum, the DPIA will contain:

1. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
3. An assessment of the risks to the rights and freedoms of the data subjects.
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned. (Note: the list provided for Data Protection by Design and Default will also be completed for the Data Protection Impact Assessment)
5. Where appropriate, NCI will seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

It is the responsibility of NCI and its designated business owners, not the DPO, to carry out DPIAs as necessary. However, the DPO shall be consulted at each stage of the DPIA, and shall provide advice and guidance as follows:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- whether or not the DPIA has been correctly carried out and whether its conclusions are in compliance with the GDPR
- whether or not prior consultation with the supervisory authority is required in line Article 36 of the GDPR following a review of the DPIA
- whether or not to go ahead with the processing following a review of the DPIA
- what safeguards to apply if processing does go ahead

All consultation with the DPO will be retained as evidence for audit purposes. Where the advice of the DPO is not taken, the Article 29 Data Protection Working Party: Guidelines on Data Protection Officers recommends that the reasons for not adhering to the advice of the DPO should be documented. NCI shall formally record these reasons in the DPIA documentation.

Further external guidance in the performance of a DPIA is provided by the following resources:

- https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- https://www.cnil.fr/en/privacy-impact-assessment-pia
- https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf
- https://www.oaic.gov.au/privacy/guidance-and-advice/10-steps-to-undertaking-a-privacy-impact-assessment-poster/

- http://www.pdp.ie/training/practical-guide-to-impact-assessments-data-protection-ireland-journal.pdf

6 Personal Data Breach Handling

6.1 What is a Personal Data Breach?

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Example of typical data breaches are:

1. Loss or theft of data or equipment on which data is stored
2. Loss or theft of documents/folders
3. Unforeseen circumstances such as a flood or fire which destroys information
4. Inappropriate access controls allowing unauthorised use
5. A hacking/cyber attack
6. Obtaining information from the organisation by deception, misaddressing of e-mails, human error, etc.

The above examples include the accidental loss of personal data as statistics indicate that most breaches are internal in nature and due to non-malicious user behaviour (e.g. loss of unencrypted laptop or USB, paper files, etc.).

6.2 How do employees report a Data Protection Breach?

In order for NCI to be able to comply with the GDPR, it is essential that all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data are reported **without delay** to the DPO using the contact details found in section 2.2 of this document. Where the DPO is unavailable, a secondary point of contact shall be identified, and the incident shall be reported in line with the agreed procedure.

In the event of a suspected personal data breach happening, employees shall notify the DPO immediately. Employees shall not assume that the DPO is already aware of the suspected breach.

6.3 How Personal data breaches will be handled in NCI

The GDPR requires that NCI:

1. *Document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance.*

NCI has developed a separate, comprehensive Data Breach Incident Procedure in order to handle data breaches in line with the requirements of the GDPR. In the event of a suspected personal data breach, a summary of the personal data breach shall be recorded in the NCI Data Breach Log as per the procedure. Each summary shall contain the facts relating to the personal data breach, its effects, and

the remedial action taken. The NCI Data Breach Log shall be maintained by the DPO. The DPO will assess the breach, and make a decision on the next steps to be taken.

Refer to the NCI Data Breach Incident Procedure for full procedures regarding:

1. Notifications to the supervisory authority
2. Notifications to data subjects
3. Notifications to controllers

All staff and contractors must familiarise themselves with the NCI Data Breach Incident Procedure.

7 THIRD COUNTRY TRANSFERS

All NCI personal data must remain within the European Economic Area (EEA). Where a business need requires the transfer or processing information outside of the EU, the NCI DPO shall be contacted for consultation.

Particular attention is required to the selection of processors when using online services, such as cloud services, for the processing of information as NCI must ensure all processing remains within the EU (e.g. online marketing surveys etc.).

8 DATA SHARING – CONTROLLER, PROCESSORS, AND THIRD PARTIES

8.1 WHAT IS OUR ROLE WITHIN NCI – DATA CONTROLLER OR PROCESSOR

The Article 29 Data Protection Working Party of the European Commission published a guidance document on the concepts of controller and processor (reference 3).

'Data controller' means:

1. the natural or legal person, public authority, agency or other body which,
2. alone or jointly with others,
3. determines the purposes and means of the processing of personal data;

The following provides 3 example scenarios within the NCI:

Scenario	**NCI**	**Third Party**
Processing of Student Personal Data	Controller	Processor (FEI)
Processing of personal data for the provision of college accommodation (TCAS)	Controller	Controller
Processing of Student Personal Data	Processor	Controller (HEA)

In most instances, NCI has been identified as the Data Controller. Where there is uncertainty regarding the designation of NCI as either controller, processor, or joint controller, the DPO shall be consulted for clarification.

8.2 What are our requirements in the use of Data Processors and how we comply with them?

Whenever NCI share personal data with a recipient outside of the Organisation, the sharing of the information must be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. This applies to all forms of sharing of information with recipients. For example, engaging the services of an external solicitor is no different to engaging the services of any other service provider. For that reason, it is unlawful for NCI to pass any personal data to an external solicitor unless NCI have put a contract in place describing the nature and purpose of processing, in addition to other specific contractual requirements as detailed in this section (the data protection principles and subject rights retained).

8.3 Evaluation of processors and pre-processing Agreements

NCI must use only processors providing sufficient guarantees to implement, and be able to demonstrate, appropriate technical and organisational measures taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

Please see **Addendum 1** for a list of standard questions which must be asked when engaging a processor, and prior to engagement of processor (used to help evaluate the suitability of the processor pre-contract). Processors must get permission to use further sub-processors – e.g. brokers.

8.4 What are our requirements as Data Controller and how we comply with them?

All processing agreements must be governed by a contract that is binding on the processor with regard to the controller and that sets out:

1. subject-matter
2. duration of the processing
3. nature and purpose of the processing
4. type of Personal data and categories of data subjects

That contract or other legal act shall stipulate, in particular, that the processor:

1. Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
2. Processes all personal data within the EU.
3. Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
4. Shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including as appropriate:

    a. the pseudonymisation and encryption of personal data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

e. the account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

5. Assist NCI by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights under data protection requirements and good practice.
6. Assists NCI in ensuring compliance with the data protection obligations taking into account the nature of processing and the information available to the processor.
7. At the choice of NCI, deletes or returns all the personal data to NCI after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.
8. Makes available to NCI all information necessary to demonstrate compliance with our data protection obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by NCI or another auditor mandated by NCI.
9. The processor shall immediately inform the controller if, in its opinion, an instruction infringes any data protection regulations, acts or good practices.
10. Where a processor engages another processor for carrying out specific processing activities on behalf of NCI, the same data protection obligations as set out in the contract between NCI and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet NCI requirements. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to NCI for the performance of that other processor's obligations.

9 ADDENDUM 1: QUESTIONS FOR PROCESSORS

Please see below a list of standard questions which must be asked when engaging a processor, and prior to engagement of processor (used to help evaluate the suitability of the processor pre-contract). Processors must get permission to use further sub-processors – e.g. brokers.

REF	REQUIREMENT
1)	NCI requires the solution to adhere to good industry security practice and must be in compliance with all applicable legislative and regulatory requirements, specifically: • NCI Policies • Legislative Requirements (e.g. EU GDPR, Data Protection Acts) NCI policies will be made available to the successful tenderer. If partially compliant, please specify explicitly the areas of non-compliance.
2)	Please confirm you will make available to NCI all information necessary to **demonstrate** compliance with data protection good practice and GDPR.
3)	The supplier must allow for, and contribute to, audits and vulnerability testing, conducted by NCI or another auditor mandated by NCI. The supplier agrees to facilitate such a technical verification test and agree to repair defects found which are as a result of not conforming to a requirement detailed in this document.
4)	Please describe all external/public interfaces to the proposed solution, in particular, those which may be accessed directly by the public.
5)	Please describe all internal and administrative interfaces to the proposed solution along with the user profiles/type of user expected to use each interface.
6)	It must be possible to trace all activity on the system through the use of an audit trail (e.g. login events/failed logins etc.). The audit trail should be timestamped and retained for a sufficient period of time to allow for the offline retention and/or enable investigation of incidents.
7)	Please describe security controls implemented on the external/public interfaces, specifying how controls are implemented to prevent (for example): a) Input validation issues such as SQL Injection, Command Injection, Cross-Site Scripting, etc. b) Authentication issues (e.g. bypassing authentication). c) Authorisation issues (e.g. ability to view or manipulate other users' data) d) Access control issues (e.g. masquerading as a different user). e) Password strength and brute-force issues (e.g. password lockout/reset issues) f) Session management issues (e.g. session predictability, hi-jacking or lack of session management, etc.) g) Parameter tampering (e.g. ability to manipulate values on the server for gain, or to gain access to unauthorised data).

	h) Administrative processes and issues (e.g. ability to escalate privileged commands or connect to the administrative interface). i) Other flaws which may result in breaches of confidentiality, integrity or availability. It is expected that best practice web application security will be applied in the solution to prevent the above issues.
8)	The solution design needs to be compliant with the data protection requirements and good practice, including: a) Secure by Design b) Secure by Default c) Pseudonymisation (where possible) d) Data Retention period enforcement e) Encryption of data at rest and in transit f) Implementation of "minimum rights" for users g) Auditing of user access Please describe how your solution **demonstrates** compliance with above (a) – (g), in particular for High Risk and Special Categories of personal data (e.g. medical or financial data).
9)	The information needs to be processed in compliance with the EU GDPR principles, including: a) Data minimisation: only process the information required. b) Accuracy: information processed needs to be reasonably kept up to date. c) Stored for only the period required: For example, should a student not complete their application process and record of the incomplete application is no longer required, how the information is removed from the solution. d) Data transfers: only transferred in line with the GDPR Please describe how your solution **demonstrates** compliance with above (a) – (c), in particular for High Risk and Special Categories of Personal data (e.g. medical or financial data).
10)	Processing of Special Categories of personal data (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), is prohibited under the EU GDPR unless explicit consent is provided. Please describe: a) All Special Categories of information proposed to be processed. b) Where the information will be stored. c) Necessity and proportionality of the information processing i.e. why it is required. d) How the solution proposes to collect explicit consent for the processing of Special Categories of personal data. e) How the solution proposes to maintain records of explicit consent for Special Categories.

11)	The subjects have a right to access, rectification, and erasure of the information. Please describe: a) How the solution supports extracting all information relating to a specific individual (in order to fulfil Subject Access Requests). b) How the solution supports erasure of all information related to a particular individual (to support the Subjects Rights to Erasure).

10 Addendum 2: Personal Data Handling Rules

In order to apply appropriate technical and organisational measures, it is necessary to classify and define handling rules for the different classifications of personal data.

10.1 Personal Data Risk Levels

At the heart of the GDPR, is an analysis of the risks from the various types of processing taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. This is based on the impact or level of damage that may be suffered by the Data Subject (as opposed to NCI).

A risk rating has been assigned to each **Personal Data Category** based on the following criteria:

Category Risk Level	Description	Information Examples
High	This category contains personal data which includes Special Categories of personal data, personal data relating to criminal convictions and offences, bank account, or payment card number details.	• Anything revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning medical or health, data concerning a natural person's sex life or sexual orientation. • Bank account or payment card details • Other information highly sensitive in nature, such as personal data relating to an individual's criminal convictions and offences
Medium	This category contains personal data which the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to the data may result in a high risk to the rights and freedoms of natural persons.	• Identification data such as social security numbers, copies of passports which may be able to identify ethnic origin, CCTV footage, etc. • Employee information including performance reviews, resumes, employee contracts or other non-Special Category data • Student information including course details, grades, assessments, and other non-Special Category data
Low	This category contains personal data which the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to the data	• All other forms of personal data including names, addresses, contact details etc.

	is less likely to result in a high risk to the rights and freedoms of natural persons.	

10.2 Data Handling Rules

The following defines the ***minimum*** handling requirements for each personal data classification. Note that all personal data (regardless of its format), may only be processed in line with data retention requirements:

Storage Item	**Low**	**Medium**	**High**
Storage on Laptops	Laptops not be used as a storage location		
Storage on public or shared work drives (e.g. network file shares)	May be stored in line with Data Retention requirements. All personal data must be restricted on need to know basis.	*Must not be stored on public or shared work drives.*	
Storage on personal work drives (e.g. personal home folder)	May be stored however should be structured in such a manner/system which ensures implementation of the Data Retention Policy.		
Email transfer Note: Email is a method of communication and must not be used as a storage location.	May be used for the transfer of information only. Email must not be considered as an area in which to store information for the long-term. Emails which are important must be saved into an appropriate storage area with other records on the same topic. This will ensure a full and complete record is kept and that emails containing personal data are not 'lost' or hard to retrieve should they be deleted or archived. A contract must be in place for all recipients with whom personal data is shared, and the sharing should be appropriately risk assessed.		
	Consider encryption of email based on risk.		Must be encrypted if transferred via email.

<table>
<tr><th>Storage Item</th><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><td>Processed within NCI structured applications (e.g. Microsoft CRM, Quercus+, etc.).</td><td colspan="2">May be stored in line with Data Retention requirements, however, data stored must be minimised, and restricted on a “need-to-know” basis.</td><td>Should not be stored unless deemed absolutely necessary and where appropriate technical and organisational controls are in place to protect the personal data.</td></tr>
<tr><td rowspan="2">Paper-based files – access control and transfers</td><td colspan="3">A contract must be in place for all recipients with whom personal data is shared, and the sharing of the data must be appropriately risk assessed.

Must be restricted on a need to know and minimum rights basis.</td></tr>
<tr><td colspan="3">Must not be stored in public/common areas.

Should not be stored or processed offsite except if there is an absolute business requirement and the risk appropriately assessed.</td></tr>
<tr><td>CCTV footage</td><td colspan="3">Must not be disclosed unless:
A contract is in place
Legally required to disclose the footage (such as official investigation by Gardai where formal, written request has been made)
Must only be reviewed by authorised persons.

Must be processed on NCI controlled systems and within NCI physical location.

Must be securely destroyed in line with recommended data retention guidelines (current recommendation is 30 days).</td></tr>
<tr><td>Everything else

(Including spoken communications etc.)</td><td colspan="3">Must not be disclosed unless a contract is in place.

Processed on NCI controlled systems and within NCI physical location.</td></tr>
<tr><td>Data destruction</td><td colspan="3">Must be securely destroyed in line with Data Retention requirements.</td></tr>
</table>

The above identifies minimum handling requirements only. Additional controls may be put in place for certain personal data types if required in addition to the above.