GENERAL DATA PROTECTION REGULATIONS (GDPR)

Guidelines and Procedures

June 2018

Table of Contents

General Data Protection Regulation (GDPR) 3

The Data Protection Acts 1988 and 2003 3

The General Data Protection Regulation 3

Principles of the Act 4

Data Protection Principles 4

Responsibility 4

Policy and Guidelines 5

Purpose of these guidelines 5

Terminology 4

Role of the Data Protection Commissioner 6

Rules of Data Protection 5

Obtaining and Processing Personal Data 6

Disclosing Personal Data 7

Permitted disclosures of Personal Data 7

Securing personal data 8

Accuracy and completeness of personal data 9

Retention of personal Data 9

Disposal of personal data 9

Rights of data subjects 9

Restriction of rights of access 9

Provision of access to third parties 10

Right of rectification or erasure 10

Responsibilities of data subjects 11

Requests for access……..12

How to Access Personal Data …… 12

Data Breach Policy……13

Purpose and Scope …… 13

Definitions/Types of Breach……13

Reporting an Incident……14

Containment and Recovery……14

Investigation and Risk Assessment ……15

Notification ……15

Evaluation and Response……15

Policy Review ……16

APPENDIX 1

Data Breach Report Form……. ……17

APPENDIX 2

Retention Schedule ……18

General Data Protection Regulation (GDPR)

The WDC is obliged to comply with the Data Protection Act, 1988 and the Data Protections (Amendment) Act 2003. This Policy outlines the WDC's commitment to protect the rights and privacy of individuals in accordance with these Acts.
The WDC needs to collect and use data for a number of reasons about its staff, Board, Committees and Stakeholders. The purposes of processing data include personal information with regard to contact details, HR, payroll, compliance with statutory obligations i.e. Code of Practice. Data protection is ensuring that the privacy rights of individuals are safe and secure when dealing with the processing of personal data.

The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 give guidance on the rights of individuals as well as the responsibilities on those persons processing personal data.

The Data Protection Acts 1988 and 2003

The collection and use of personal data are primarily governed in Ireland by the Data Protection Acts 1988 and 2003. The consolidated Acts implement the corresponding EC Directive on the protection of the individuals with regard to the processing of personal data and on the free movement of such data (95/46/EEC)

The General Data Protection Regulation

The EU's legislative bodies negotiated from 2011 – 2015 in order to prepare an updated and more harmonised data protection law for Europe. The General Data Protection Regulation (GDPR) is a European Union Regulation that has been designed to strengthen and unify Data Protection within the EU. The GDPR came into effect on 25th May 2018.

The new GDPR practices will update and harmonise data protection law for the EU much of the emphasis will be on transparency, security and accountability by data controllers and processors. It will also standardise and strengthen the right of the EU citizens to privacy of their personal data.

The WDC website will be updated on a regular basis with further developments over the coming months.

GDPR Regulations can be accessed **Here.**

The New Data Protection Bill 2018 has been published and can be viewed **Here.**

Another useful website developed by the Data Protection Commissions can be found here **"GDPR and You"**

Principles of the Act

Data Protection Principles

The WDC will adhere to its responsibilities under the legislation in accordance with the eight data protection principles outlined in the Act as follows:

1. Obtain and process personal data fairly and lawfully, and not unless one of the legitimising conditions in Section 2A (see below) applies (for personal data) or and Section 2B (see below)applies (for sensitive personal data).
   S.I. No. 220/2016 - Data Protection Act 1988 (Section 2A) Regulations 2016.
   S.I. No. 426/2016 - Data Protection Act 1988 (Section 2B) Regulations 2016.

2. Obtain data for one or more specified, explicit and lawful purposes. Only use and disclose data in ways compatible with those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose for those purposes.

5. Personal data processes shall be accurate and, where necessary, kept up to date.

6. Personal data shall be processed in accordance with the rights of individuals.

7. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

8. Personal data shall not be transferred outside the European Economic Area (EEA) or any safe countries without relevant safeguards being met.

Responsibility

The WDC has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of the WDC who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. The WDC will provide support, assistance, advice and training to all staff to ensure it is in a position to comply with the legislation. The WDC has appointed a Data Protection Officer who will assist the WDC and its staff in complying with the Data Protection legislation.

Policy and Guidelines

This policy supports the provision of a structure to assist in the WDC's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

The purpose of the Act is to safeguard the privacy rights of individuals regarding the processing of their personal data by those who control such data. It provides for collection and use of data in a responsible way, whilst also safeguarding against unwanted or harmful use of that data.

Purpose of these guidelines

The purpose of these procedures is to assist employees of the WDC in supporting the organisation's Data Protection Policy which outlines its commitment to protect the privacy rights of individuals in accordance with the legislation. These guidelines set out the areas of work in which data protection issues arise and outline best practice in dealing with these issues.

Terminology

"Personal Data" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition is – deliberately - a very broad one. In principle, it covers any information that relates to an identifiable, living individual. However, it needs to be borne in mind that data may become personal from information that could likely come into the possession of a data controller.

There are different ways in which an individual can be considered 'identifiable'. A person's full name is an obvious likely identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms occupation, address etc.

The definition is also technology neutral. It does not matter how the personal data is stored – on paper, on an IT system, on a CCTV system etc.

" Processing" means any operation or set of operations which is performed upon personal data or sets of 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.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

"Data Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU law or Irish law, the controller or the specific criteria for his nomination may be designated by EU law or by Irish law.

"Data Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Role of the Data Protection Commissioner

The Data Protection Commissioner (DPO), with whom the WDC is registered as a data controller oversees compliance with the terms of legislation. The Commissioner has a wide range of powers including investigation of WDC records and record-keeping practices. A data controller found guilty of an offence can be fined up to €100,000 and/or may be ordered to delete data.

Rules of Data Protection

There are eight rules of data protection, which govern the processing of personal data. When processing personal data the following procedures apply:

1. obtain and process the data fairly;
2. keep only for one or more specified and lawful purposes;
3. use and disclose only in ways compatible with the purposes for which it was initially given;
4. keep safe and secure;
5. keep accurate and up-to-date;
6. ensure that it is adequate, relevant and not excessive;
7. retain no longer than is necessary for the specified purpose or purposes;
8. provide a copy of his/her personal data to any individual, on request.

In addition, there are special conditions that must be met before personal data may be transferred to a country outside the European Economic Area (E.U. member states and Iceland, Liechtenstein and Norway) if that country does not have an EU-approved data protection law. Specific provisions are in place concerning personal data transfers to the United States of America.

The above rules apply to all personal computer held data and to all personal manual data created from the 1st July 2003. For personal manual data created before the 1st July 2003, the first seven rules outlined above will apply from the 24th October 2007. Until that date the following procedures apply:

1. provide a copy of his/her personal data to any individual on request;
2. correct, erase, or destroy any manual personal data that are incomplete or inaccurate;
3. destroy any personal manual data that are incompatible with the legitimate purpose for which they were collected.

The WDC must observe the following procedures at all times to be fully compliant with these rules:

Obtaining and processing personal data

Personal data is obtained fairly if the data subject is aware of the purpose for which the WDC is collecting the data, of the categories of person/organisation to whom the data may be disclosed, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data.

- Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data are necessary for fulfilling that purpose and ensure data are used only for that purpose.
- It follows that use of WDC data processing facilities in capturing and storing personal data for non-WDC purposes must not take place.
- Inform data subjects of what personal information is held by the WDC, what it will be used for and to whom it may be disclosed.
- Obtain explicit consent in writing for processing sensitive data and retain a copy of that consent. Consent cannot be inferred from non-response in the case of sensitive data.

Disclosing personal data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of sensitive personal data, the disclosure of which would normally require explicit consent.

- Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.
- Verbal consent to disclosure of personal data to the data subject may be obtained by telephone in the case of non-sensitive personal data, but must include asking the subject to confirm facts that should be known only to them, such as date of birth, address, etc. The date and time of the giving of the verbal consent should be recorded in writing.
- Verbal consent to disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the Gardaí for example, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject.
- Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions. Be satisfied of the need to disclose.
- Personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract, to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

Permitted disclosures of personal data

The Act provides for disclosures, where data are:

- authorised for safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- required to protect the international relations of the State;
- required urgently to prevent damage to health or serious loss/damage to property;
- required under law;
- required for legal advice or legal proceedings;
- disclosed to the data subject;
- disclosed at the request or with the consent of the data subject.

Securing personal data

The WDC must protect personal data from unauthorised access when in use and in storage and must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to stringent controls, passwords, encryption, access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.
- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, ensure the hard drive is cleaned by the IT Provider.
- Special care must be taken where laptops and PCs containing personal data are used outside the WDC.
- A Data controller disclosing personal data to a data processor should do so under a written contract specifying security rules to be followed.

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data is accurate, complete and kept up-to-date. Review and audit procedures should be in place to monitor that this is being achieved.

Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which they were collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose. Personal information should only be held for periods specified in the WDC Retention Schedule.

Disposal of personal data

Personal data should be disposed of when it is no longer needed for the effective functioning of the WDC and its staff. The method of disposal should be appropriate to the sensitivity of the data e.g. shredding, incineration in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs are transferred from one person to another or outside the WDC or are being disposed of.

Rights of data subjects

Right of access

The Act provides for the right of access by the data subject to his or her personal information. Data subjects must be made aware of how to gain access to their personal data. A data subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A data subject is entitled to the following information on written application within forty days:

- A copy of his or her personal data;
- the purpose of processing the data;
- the persons to whom the WDC discloses the data;
- an explanation of the logic used in any automated decision-making;
- a copy of recorded opinions about him or her, unless given in confidence.
- A maximum fee of €6.35 may be charged.

Restriction of rights of access

The right of access is restricted where the data are:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- subject to legal professional privilege;
- kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;
- back-up data.

Provision of access to third parties

A data subject is entitled to access his or her own personal data only. The personal information of a data subject including contact details must not be disclosed to a third party, potential employer, employer, professional body etc., without the consent of the individual concerned. An agreement may be made to forward a communication to a data subject on behalf of a third party, but no information should be disclosed about the data subject. In the case of research surveys where there is an agreement to forward documentation to data subjects, a notice should be included to the effect that no personal information has been released.

Limitations on the use of personal data for research.

All researchers involved in collecting personal data, especially sensitive personal data, must comply with the requirements of the Act.

Initially, they must ensure that data are obtained and processed fairly. It is essential that the necessary consent from data subjects is obtained. Whenever possible, personal data should be rendered anonymous.

The Act requires that personal data shall be kept only for one or more specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those. This restriction may limit the usefulness of data for research purposes. If personal data is made anonymous, however, it ceases to be personal data subject to the terms of the Act.

In addition, certain data protection rules are relaxed for personal data kept for statistical, research or other scientific purposes, so long as the data are not used in a way that may harm the data subject. The rules in question being the restrictions on further processing personal data which is incompatible with the original purpose and on not keeping data longer than necessary for the purpose and on not disclosing the purpose when the data was obtained. It should be noted that if research data is retained in personally identifiable format it may be subject to an access request from a data subject and is subject to restrictions on the transfer of data outside the European Economic Area.

Right of rectification or erasure

Data subjects have a right to have personal data rectified, blocked from being processed or erased where the data controller has contravened the Act.
In order to comply with the above rights of access, rectification or erasure, ensure that personal data can be located and collated quickly and efficiently as follows:

- Ensure personal data is in a format that is easy to locate and collate.
- Verify that the access request and the personal data released refer to the same individual.
- Know exactly what data is held on individuals, and by whom.
- Hold personal data in a secure central location.

Responsibilities of data subjects

All staff, and other data subjects are entitled to be informed how to keep their personal data up to date. All staff and other data subjects are responsible for:

- checking that any information that they provide to the WDC is accurate and up to date
- informing the WDC of any changes of information, which they have provided, e.g. changes of address
- checking the information that the WDC will send out from time to time, giving details of information kept and processed
- informing the WDC of any errors or changes (the WDC cannot be held responsible for any errors unless previously informed).

Further information can be obtained from:

The Data Protection Officer
Western Development Commission
Dillon House
Ballaghaderreen
Roscommon
F45 WY26

Phone: 094 9861441
E-mail: dataprotection@wdc.ie

Requests for access

Under the Data Protection Acts, you have the right to be given a copy, clearly explained, of any of your personal data kept on computer or manual relevant filing systems simply by making a written request.

If you wish to access your personal data held by the WDC you should contact the Data Protection Officer in the first instance and check if the data can be released routinely.

If this is not possible you can make an application under the Data Protection Act 1988 and (Amendment) Act 2003.

You must write a letter clearly stating that you are applying under the Data Protection Acts. All applications should be addressed to:

The Data Protection Officer,
Western Development Commission
Dillon House
Ballaghaderreen
Co. Roscommon
F45 Y26
E-mail: dataprotection@wdc.ie

To help us answer your request please be as specific as possible about the information you wish to see, and give as much information as you can to help us find it.

You are legally entitled to a decision regarding your request **within 40 days** of the WDC receiving your request. However every effort will be made by the Data Protection Officer to deal with your request as soon as possible. You will be asked to provide proof of your identity.

If you are unhappy with the decision of the Data Protection Officer you have the right to complain to the Data Protection Commissioner who will investigate the matter for you. The Commissioner has legal powers to ensure that your rights are upheld.

Further details on your rights under the Data Protection Acts are available at the Data Protection Commissioners website www.dataprivacy.ie.

Address:
Office of the Data Protection Commissioner
3rd Floor, Block 6
Irish Life Centre
Lower Abbey Street
Dublin 1
Telephone: + 353 1 874 8544
E-mail: info@dataprivacy.ie

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 by the company (including any temporary or permanent loss of control of, or inability to access, personal data.

The WDC collects, holds, processes, and shares personal data, a valuable asset that needs to be protected. Every care is taken to protect personal data from incidents (either accidently or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

Purpose and Scope

The WDC is obliged under the Data Protection legislation to have in place an organisational framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

- This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the WDC.
- This policy relates to all personal and commercially sensitive data held by the WDC regardless of format
- This policy applies to all staff of the WDC including Board Members, Management, staff, temporary or casual, contractors, consultants, suppliers and data processors working for or on behalf of the WDC
- The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definitions/Types of Breach

For the purposes of this Policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the WDC's information assets and/or reputation.

An incident includes but is not restricted to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB Stick, iPad/Mobile phone, tablet or paper record);

- Equipment theft or failure;
- System failure;
- Unauthorised use of, access to or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to Information or IT Systems;
- Website defacement;
- Hacking attack;
- Unforeseen circumstances such as a fire or flood;
- Human error;
- Offences where information is obtained by deceiving the organisation who holds it.

Reporting an Incident

Any individual who accesses, uses or manages the WDC's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer at dataprotection@wdc.ie

If the breach occurs or is discovered outside normal working hours it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Log should be completed as part of the reporting process (See Appendix 1)

All staff should be aware that any breach of Data Protection legislation may result in the WDC Disciplinary Procedures being instigated.

Containment and Recovery

The Data Protection Officer (DPO) will, in the first instance, determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

- An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach, in some cases it could be the DPO or the Chief Executive Officer (CEO) of the organisation.

- The DPO/CEO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

- The DPO/CEO will establish who may need to be notified as part of the initial containment and will inform the relevant authorities where appropriate (e.g. Garda

Síochána).

- The DPO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and Risk Assessment

An Investigation will be undertaken by the DPO/CEO immediately and wherever possible, within 24 hours of the breach being discovered/reported. The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- The type of data involved; Its sensitivity;
- The protections are in place (e.g. encryptions);
- What has happened to the data (e.g. has it been lost or stolen;
- Whether the data could be put to any illegal or inappropriate use;
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);

Notification

The DPO/CEO, in consultation with relevant colleagues will establish whether the Office of the Data Commissioner will need to be notified of the breach, and if so, notify them **within 72 hours** of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis, however the following will need to be considered:

- whether the breach is likely to result in a high risk of affecting individuals rights and freedoms under Data Protection legislation;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal/contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedom, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved.

Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided

with a way in which they can contact the University for further information or to ask questions on what has occurred.

The DPO/CEO must consider notifying third parties such as the Garda Síochána, insurers, banks or credit card companies and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The Review will consider:

- Where and how personal data is held and where and how it is stored;
- Where the biggest risks lie including identifying potential weak points within existing security measures;
- Whether methods of transmission are secure; sharing minimum amount of data necessary;
- Staff awareness;
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by University Executive Committee.

Policy Review

These Policies and Guidelines will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

This Policy was approved by the WDC Board in May 2018.

APPENDIX 1

Data Breach Report Form

Data Breaches should be reported promptly. If you discover a data breach, please notify the Chief Executive Officer (CEO) immediately, complete Section 1 of this form and e-mail it to the Data Protection Officer (DPO) at dataprotection@wdc.ie

SECTION 1: Notification of Data Security Breach	**To be completed by person reporting incident**
Date the incident was discovered:	
Date(s) of Incident:	
Place of Incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If so, please provide details:	
Brief Description of any action taken at the time of discovery:	
For use by the Data Protection Officer (DPO)	
Received by:	
On (Date):	
Forwarded for action to:	
On (Date)	

SECTION 2: Assessment of Severity	To be completed by the DPO in consultation with the CEO and if appropriate IT (if it is an IT Breach)
Details of Information Loss:	
What is the nature of the information loss?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT Server	
Is the information unique? Will its loss have adverse operational, research, financial, legal liability or reputational consequences for the WDC or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please forward details of any types of information that fall into any of the following categories:	
HIGH RISK: **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual: (a) racial or ethnic origin; (b) political opinions or religious beliefs; (c) trade union membership; (d) genetics; (e) biometrics (where used for ID purposes); (f) health; (g) sex life or sexual orientation	
▪ Information that could be used to commit identify fraud such as, personal bank account and other financial information, national identifiers such as PPS Number and copies of passports or visas;	
▪ Personal information relating to vulnerable adults and children;	
▪ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
▪ Security information that would compromise the safety of individuals if disclosed;	
DPO/CEO to consider whether it should be escalated to the WDC Board.	

SECTION 3: Action Taken	To be completed by DPO/CEO
Incident Number	e.g. Year/001
Report Received by:	
On (Date):	
Action taken by responsible officer(s):	
Was incident reported to Garda Sícohána?	Yes/No If YES, notified on (Date):
Follow up action required/recommended	
Reported to the DPO on (date):	
Reported to other internal stakeholders (details, dates etc.):	
For use of DPO and/or CEO	
Notification to Data Protection Commissioner (DPC)	Yes/No If YES, notified on (Date): Details:
Notification to other external regulator/stakeholder	Yes/No If YES, notified on (Date): Details:

Appendix 2:

RETENTION SCHEDULE

Description	Retention	Timeframe	Dispose/Delete
Corporate			
Board Minutes of Meetings - Hard and Soft Copy	Current	Indefinitely	
Internal Audit Minutes of Meetings - Hard and Soft Copy	Current	6 years	Confidential Disposal
Dept. Circulars	Current	12 months	Dispose
Dept. Correspondence - Hard Copy and Soft Copy	Current	12 months	Confidential Disposal
Finance Files - Financial Statements - WIF Loans - EU Projects	Current	7 Years	Confidential Disposal
Minutes of Adhoc Meetings	Current	12 months	Confidential Disposal
HR - Personnel Files - Contracts of Employment - All Leave/Holiday Records - Contact Details - Salary/Revenue Details - Grievance/Disciplinary	Current Current Current Current Current	Annual Review + 8 yrs 3 Years Annual Review + 8 yrs Annual Review + 8 yrs 12 Months	Confidential Disposal
Recruitment Files (Unsuccessful) Recruitment Files (Panel)	Current Current	6 months 6 months	Confidential Disposal
WDC General (post, reports)	Current	12 months	Dispose
WDC Tenders/RFQ's/RFT's	Current	Archive 6 years	Confidential Disposal
E-mails – Department - Auditors, - PQ's, - Board - General	Current	Annual Review	Delete
Supplier Contracts	Current	6 Years	Confidential Disposal
Office/Building Insurance	Current	Annual Review	Dispose
FOI Requests	Current	12 months	Confidential Disposal

Data Protection Requests	Current	12 months	Confidential Disposal
Corporate Governance - Ethics in Public Office - Designated Positions of Employment -Statements of Interest	Current	6 years	Confidential Disposal
WDC Website	Current	Annual Review	Update/Delete
Western Investment Fund			
FAP Minutes	Current	Indefinitely	
WIF Investments	Current	6 Years	Confidential Disposal
WIF - unsuccessful applications	Current	12 Months	Confidential Disposal
WIF – Decommittals	Current	12 months	Confidential Disposal
EU Projects			
Documentation for EU Projects	Current	7 Years	Confidential Disposal
RFQ's/RFT's/e-Tenders	Current	7 Years	Confidential Disposal
Finance	Current	7 Years	Confidential Disposal
E-mails	Current	Annual Review	Delete
Policy			
Reports/Blogs/Insights/e-zine	Current	12 Months	Dispose
RFQ's/RFT's/e-tenders	Current	7 Years	Confidential Disposal
E-mails	Current	Annual Review	Delete
Finance	Current	7 Years	Confidential Disposal
Regional Development			
Lookwest.ie – Website	Current	Annual Review	Update/Delete
RFQ's/RFT's/e-tenders	Current	7 Years	Confidential Disposal
Finance	Current	7 Years	Confidential Disposal
E-mails	Current	Annual Review	Delete
EU Project Documentation	Current	7 Years	Confidential Disposal

Note: Please ensure that all soft copies relating to any hard copy disposals are also deleted from the Server – e.g. documents stored on the shared drive and/or outlook