General Data Protection Policy

Document Control			
Policy Owner	Head of IT, Barry O'Hagan		
Policy Author	Head of IT, Barry O'Hagan		
Version	2.0		
Consultation	Senior Management Team Yes Trade Unions Yes		
Equality Screened by	Yes	**Date**	
Equality Impact Assessment	N/A	**Date**	
Good Relations	Yes or No or N/A		
Approved By	(Policy & Resources)	**Date**	March 2021
Adopted By	Council	**Date**	March 2021
Review Date	24 months from date of Adoption	**By Whom**	Head of IT & DPO
Circulation	Councillors, Staff, Intranet		
Document & legislation Linkages and	Internet policy Mobile Phone Policy Email and Instant Messaging Policy The Privacy and Electronic Communications Regulations (PECR) Regulation of Investigatory Powers Act 2000 Lawful Business Practice Regulations,. Home (Remote Working Guidance) And Policy(draft)		

CONTENTS PAGE (to be finalised last)

1.0 INTRODUCTION

The new Data Protection Act 2018 (DPA) replaces the old data protection legislation and came into force on 25th May 2018.

The 2018 Act modernises data protection laws in the UK to make them fit-for-purpose for our increasingly digital economy and society. As part of this, the 2018 Act applies the EU's GDPR standards, by having strong data protection laws and appropriate safeguards.

The legislation is ensuring that modern, innovative uses of data can continue. At the same time, it has strengthened the controls and protection individuals have over their data.

The data protection principles set out the main responsibilities for the Council.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Poor practice or a serious breach could not only harm individuals but would also have a serious effect on the reputation, employees and the financials of the Council.

2.0 POLICY AIM & OBJECTIVES

2.1 **Policy Aim**:

i. To provide assurance to our employees and public that we seek to protect the information we hold and used it for legitimate purposes.

ii. To ensure Council meets the requirements of the General Data Protection Act 2018

iii. To ensure that all appropriate staff are properly trained, kept fully informed of their obligations under the Data Protection Act 2018, and that they are aware of their personal data protection liabilities, setting out the standards expected by the Council in relation to processing of personal data and safeguarding individuals' rights and freedoms.

2.2 **Policy Objectives:**

To ensure the protection of personal and sensitive information of staff and our customers.

To ensure all staff across the Council are aware of, and understand the importance of, data protection and confidentiality.

To assist the Council to comply with all requirements of the DPA.

To ensure procedures are in place across the Council for staff, contractors and members regarding disclosure of personal information.

To increase the awareness of data subjects to the amount of personal data processed and stored by the Council about them and advise them of their rights under the data protection legislation.

To ensure all staff receive appropriate data protection training, with regular updates or when significant data protection guidance changes.

3.0 POLICY SCOPE

This policy applies to

- all employees(substantive and temporary) of Mid Ulster District Council
- any individual including contractors, volunteers and others who work on behalf of the Council
- all work experience and other students
- Councillors

This policy outlines the behaviours and responsibilities expected in order to ensure the Council continues to fulfil its obligations under the Data Protection Act 2018 and their related and all subsequent Data Protection legislation.

Key Definitions

It applies to all data that the Council holds relating to identifiable individuals,
This can include:

Personal information	**Special category personal data**
	Special category data is personal data, which GDPR considers sensitive and deserving of extra attention:
First name & family name or surname	racial or ethnic origin
address	religious or other philosophical beliefs
telephone numbers	political opinions
date of birth	trade union membership
age	physical or mental health or condition
qualifications	sexual orientation.
training records	offences (including alleged offences)
financial information	processing of genetic data
licensing information	processing biometric data for the purposes of identifying a natural person
enforcement action	health data
complaint information	

This list is intended as a guide and is not exhaustive.

'Controllers' and 'Processors'?
Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

If you exercise overall control of the purpose and means of the processing of personal data – ie, you decide what data to process and why – you are a controller.

If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data.

Processors act on behalf of, and only on the instructions of, the relevant controller.

Joint controllers must arrange between themselves who will take primary responsibility for complying with GDPR obligations, and in particular transparency obligations and individuals' rights. They should make this information available to individuals.

However, all joint controllers remain responsible for compliance with the controller obligations under the GDPR. Both supervisory authorities and individuals may take action against any controller regarding a breach of those obligations.

4.0 LINKAGE TO CORPORATE PLAN

With reference to Mid Ulster District Council's Corporate Plan 202-2024, this policy contributes toward the vision of professional and trustworthy services and contributes to the delivery of the Corporate Theme 'Delivering for our people' : 1.1 High performing services focused on customer need and value for money.

5.0 DATA PROTECTION PRINCIPLES

5.1 The legislation places a responsibility on every data controller(Council) to process any personal data in accordance with the eight principles. More detailed guidance on these principles can be found in the link to the ICO's website (www.ico.gov.uk).
In order to comply with its obligations, Mid Ulster District Council undertakes to adhere to the eight principles:

5.11) Process personal data fairly and lawfully.
Council will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

5.12) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.
Council will ensure that the reason for which it collected the data originally is the only reason for which it processes the data, unless the individual is informed of any additional processing before it takes place.

5.13) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.
Council will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms and mechanisms for collecting data will always be drafted with this mind.

5.14) Keep personal data accurate and, where necessary, up to date.
Council will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Council if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Council to ensure that any notification regarding the change is noted and acted on.

5.15) Only keep personal data for as long as is necessary.
Council undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Council will regularly review the information held and destroy it in accordance with its information retention schedule. Council will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

5.16) Process personal data in accordance with the rights of the data subject under the legislation.
Individuals have various rights under the legislation including a right to:

- be told the nature of the information the Council holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

Council will only process personal data in accordance with individuals' rights.

5.17) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
Council will ensure that all personal data is accessible only to those who have a valid reason for using it.
Council will implement appropriate and reasonable measures , these may include

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf; (See Section 5.9 Data Sharing Agreements & Contracts)
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer; and
- adhering to relevant codes of conduct and signing up to certification schemes.

5.18) Ensure that no personal data is transferred to a country or a territory outside

the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.2 Our legal basis for using personal data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, even deleting it – will have an acceptable legal basis. There are six of these:

- Where it involves the exercise of a public function – i.e. most activities of most government, local government and other public bodies.
- Where it is *necessary* in connection with a contract between the Council and the individual.
- Where it is *necessary* because of a legal obligation.
- Where it is *necessary* in our legitimate interests, as long as these are not outweighed by the interests of the individual.
- Where it is *necessary* in an emergency, to protect an individual's 'vital interests'.
- Consent from the individual (or someone authorised to consent on their behalf).

Where we are basing our processing on consent we will be able to 'demonstrate' that we hold consent.

Council will ensure that any data collection is transparent and the individual will be aware of the purpose for same , e.g. in a short statement on a form(fair collection statement) explaining the use of that data etc.

5.3 Disclosure of Data

Only disclosures which have been notified under the Council's privacy notices and therefore staff should exercise caution when asked to disclose personal data held on another individual or third party.
Council undertakes not to disclose personal data to unauthorised third parties, but legitimate disclosures may occur e.g.:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the ICO and is in the legitimate interests of the Council.
- the disclosure is required for the performance of a contract.
- There are other instances when the legislation permits disclosure without the consent of the individual,(see ICO or DPO for further guidance)

In no circumstances will Council sell any of its databases to a third party.

5.4 Rights of the Individual

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access (Subject Access Rights SARS)
- The right to rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The right to be Informed

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.

The Right of Access (Subject Access Rights SARs)

Individuals have a right to access any personal data relating to them which are held by the Council. Any individual can exercise this right verbally or in writing to the Data Protection Officer(DPO). (see appendix 1).
Any such request to access personal data is called a Subject access request. Any member of staff receiving a SAR should forward this to the DPO.
Under the terms of the legislation, any such requests must be responded to within one month of receipt.

In most cases Council cannot charge a fee to comply with a subject access request but where the request is manifestly unfounded or excessive Council may charge a “reasonable fee” for the administrative costs of complying with the request.

The Council will ask for information necessary to confirm the identity of the requester.

Requested personal data will be retrieved from the relevant department and screened by the DPO before completion within a month of receipt. Failure to meet SAR timescales will expose the council to risk of fines and further action from the ICO.

The right to rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing which Council must respond to within one calendar month to respond to a request. In certain circumstances you can refuse a request for rectification

The right to erasure

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances.
Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);

- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

The right to restrict processing

Individuals have the right to restrict the processing of their personal data in certain circumstances i.e. limit the way that an organisation uses their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

The right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

The right to data portability only applies when:

- your lawful basis for processing this information is consent **or** for the performance of a contract; and
- you are carrying out the processing by automated means (ie excluding paper files).

The right to object

The DPA (2018) gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data.
An objection may be in relation to all of the personal data you hold about an individual or only to certain information. It may also only relate to a particular purpose you are processing the data for.

Rights in relation to automated decision making and profiling

The GDPR applies to all automated individual decision-making and profiling.
Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

5.5 Council Marketing

The Council may hold and process some personal data for marketing purposes, e.g.
Customer information for arts and cultural programmes and other events
Photographs for use in printed and online promotional activity.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted Council access only. Therefore, it is Council policy to offer an opportunity to opt-in for marketing purposes when collecting the information.

5.6 Email

It is the policy of Council to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Council's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the Council may be accessed by someone other than the recipient for system management, security purposes and other reasons as set out in the email and instant messaging policy.

5.7 CCTV

There are some CCTV systems operating within Council and town centres for the purpose of protecting the Public and or Council property. Council has carried out privacy impact assessments in respect of these installations and will only process personal data obtained by the CCTV system in a manner which ensures compliance with our policy and applicable legislation.

5.8 Breach of Personal Data

Any incident or action that affects the confidentiality, integrity or availability of personal data could potentially be a breach that Council may have to report to the ICO within 72 hours of becoming aware of it. Such reports will be sent to the ICO using appendix 4 in accordance with their latest guidelines.

In short, there will be a personal data breach whenever

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation.
- or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Notification Requirement: such incidents must be brought to any member of the team in accordance with procedures defined in appendix 2. Council must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.(See appendix 2 for further details).

5.9 Data Sharing Agreements & Contracts

Whenever a controller uses a processor, there must be a written contract (or other legal act) in place.
The contract is important so that both parties understand their responsibilities and liabilities.
(Please contact the DPO or legal services for information and the appropriate data sharing contracts for your scenario.).
The GDPR sets out what needs to be included in the contract.
If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

The Council will use data sharing agreements to ensure all responsibilities and liabilities are addressed for each party. For more information on data sharing agreements please contact legal services or the DPO.

Council officers will use predefined template agreements inline with the guidance and the current legal advice at that time.

6.0 ROLES AND RESPONSIBILITIES

6.1 The Chief Executive is ultimately responsible for our compliance with data protection legislation.

As a public authority as defined under the legislation the Council has appointed a Data Protection Officer (see appendix 1)
The DPO's minimum tasks are defined as:

- to inform and advise the controller, its employees, and any associated processors about their obligations to comply with the GDPR and other relevant data protection laws such as Part 3 of the Bill;
- to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

Senior Management Team
The Senior Management Team are responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the Council.

Compliance with the legislation is the personal responsibility of all members of the Council who process personal information. Potential breaches of this policy will be investigated and subject to Mid Ulster District Council's or other relevant disciplinary procedure.

Heads of Service and Managers

Managers within every service or business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties.

SMT &Managers must contact the DPO or Solicitor if they are unsure about any aspect of the DPA requirements including

- what security or other measures they need to implement to protect personal data.
- the lawful basis which they are relying on to process personal data
- consent matters for processing personal data
- privacy notices or other transparency information
- the retention periods.
- the transfer of personal data outside the European Economic Area (EEA)
- engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (by Design and by Default)
- to use personal data for purposes other than those for which it was originally collected
- activities involving automated processing.
- help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors)
- sharing data with another organisation or person in a way which is new or could affect data subjects' rights.
- Any potential or suspected breach or incident relating to personal data.(see Appendix 2)

All Staff

Everyone working for us or on our behalf is required to comply with this policy.
Everyone working for us or on our behalf is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of personal data and support us in complying with data protection legislation.

Staff who handle personal data will be required to complete mandatory data protection training.

Elected Members

Members Elected members will endorse the policy, its implementation and procedures.

Compliance

We will regularly review monitor and audit the systems and processes under our control to ensure they comply with this policy. We will investigate any alleged breach of this policy in line with the breach process in Appendii 2&3 and assess whether the incident is reportable to the ICO using Appendix 4. An investigation could result in us taking action up to and including dismissal; removal from office; or, termination of a contract for services.

7.0 IMPACT ASSESSMENTS

7.1 Equality Screening & Impact

7.2 The policy has been subjected to equality screening in accordance with the Council's screening process. The outcome of the screening has screened this policy out.

7.3 Rural Needs Impact

The policy has been subjected to a rural needs impact assessment and this policy has considered the assessment during the policy development.

7.4 **Staff & Financial Resources**

This policy requires resources to train those staff handling personal data. Online E Learning and class based learning may be used. The council will assign sufficient resources to accommodate these training requirements.
No issues have been identified which would significantly impact on the Councils resources and delivery of its business as a result of this policy being implemented.

7.5 **Risk**

The risks associated with personal data legislative compliance will be recorded and reviewed in accordance with the Council's corporate risk management system by the policy Author.

8.0 SUPPORT AND ADVICE

8.1 Advice and guidance on the implementation of this should be sought from the DPO or Council solicitor and from the Information Commissioner's website at www.ico.org.uk.

9.0 COMMUNICATION

9.1 Council will ensure that all staff processing personal data receive required training on data protection.
Council will ensure that those who are responsible for implementing this policy, or responding to subject access requests under this policy, will receive additional training and resources to help them understand and to comply with them.

9.2 This policy will be published on the Intranet and brought to the attention of all staff within the Council.

10.0 MONITORING & REVIEW ARRANGEMENTS

10.1 Implementation of this policy will be monitored and a formal review undertaken 24 months from its effective date.

Appendix 1

Mid Ulster District Council

Data Controller Name: Mid Ulster District Council

Address: c/o Dungannon Office, Circular Road, Dungannon, BT71 6DT

Telephone: 03000 132 132

Data Protection Officer Name: Barry O'Hagan

Telephone: 03000 132 132

Email: barry.ohagan@midulstercouncil.org

Council's Data Protection Registration reference: **ZA086387**

Appendix 2

Data Breach Procedure and Response Plan

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation.
- or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Notification Requirement: when a security incident takes place, Council must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Alert Response

The data breach process is initiated when anyone notices that a suspected or alleged or actual data breach occurs. The DPO or any member of the Data Breach Response team must be notified as soon as possible and not later than 24hrs from becoming aware .

The data response team is made up of ;

The Data Protection Officer

Director of Finance

Any member of the IT team

Where a privacy data breach is known to have occurred (or is suspected) any member of response team staff who becomes aware of this must, within 24 hours, alert a member of data response team in the first instance.

The Information that should be provided (if known) at this point includes:

- When the breach occurred (time and date)
- Description of the breach (type of personal information involved)
- Cause of the breach (if known) otherwise how it was discovered
- Which system(s) if any are affected?
- Which directorate/faculty/institute is involved?
- Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

A template can be found at **Appendix 3** to assist in documenting the required information.

Assess and determine the potential impact.
Once notified of the information above, the team must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The DPO should be contacted for advice.

Primary role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

•Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.

•Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined above.

•Call upon the expertise of, or consult with, relevant staff in the circumstances.

•Engage an independent cyber security or forensic expert as appropriate.

•Assess whether serious harm is likely

•Make a recommendation to the DPO whether this breach constitutes a Notifiable incident for the purpose of mandatory reporting to the ICO and the practicality of notifying affected individuals. Consider developing a communication or media strategy in conjunction with the marketing and communications team including the timing, content and method of any announcements to staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The DPO will provide periodic updates to the Chief Executive and or deputy as deemed appropriate.

Appendix 3

Data Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Contact Information for this Incident	
Name:	
Title:	
Work Phone:	
Mobile Phone:	
Email address:	

2. Incident Description.

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

☐ Loss / Compromise of Data	☐ Other Organisations' Systems Affected
☐ Damage to Systems	☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ System Downtime	☐ Violation of legislation / regulation
☐ Financial Loss	☐ Unknown at this time

Provide a brief description of the impact:

Provide a brief description of data that was compromised:
5. Who Else Has Been Notified?
Provide Person and Title:
6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken ☐ System Disconnected from network ☐ Updated virus definitions & scanned system	☐ Restored backup from tape ☐ Log files examined (saved & secured) ☐ Other – please describe:

Provide a brief description:

7. Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please submit this completed form to :Head of IT

Barry.ohagan@midulstercouncil.org

Appendix 4

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ○ Initial report
- ○ Follow-up report

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ◉ I consider the incident meets the threshold to report
- ○ I do not consider the incident meets the threshold to report, however I want you to be aware
- ○ I am unclear whether the incident meets the threshold to report

About the breach

Please describe what happened

Please describe how the incident occurred

How did the organisation discover the breach?

What preventative measures did you have in place?

Was the breach caused by a cyber incident?

- ○ Yes
- ○ No
- ○ Don't know

When did the breach happen?

Date: Time:

When did you discover the breach?

Date: Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data, eg coordinates
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults

☐ Other (please give details below)

Potential consequences of the breach

Is the personal data breach likely to result in a high risk to data subjects?

- ○ Yes
- ○ No
- ○ Not yet known

Please give details

(Cyber incidents only) Recovery time

- ○ We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ○ We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ○ We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- ○ We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- ○ Yes
- ○ No
- ○ Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Have you taken actions to contain the breach? Please describe these remedial actions

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ○ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ◉ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- ○ Yes
- ○ No
- ○ Don't know

If you answered yes, please specify

About you

Organisation (data controller) name

Registration number

If not registered, please give exemption reason

Business sector

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name:

Email:

Phone:

Sending this form

Initial report
If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report
If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.

Comhairle Ceantair Lár Uladh Mid Ulster District Council

Equality & Good Relations Screening Report (updated 2019)

Introduction

Mid Ulster District Council has a statutory duty to screen its policies, procedures, practices/decisions. This Policy Screening Form and Report assists Council Departments to consider the likely equality and good relations impacts of the aforementioned, if any, placed upon our ratepayers, citizens, service users, staff and visitors to the district.

Section 1 – Policy scoping

This asks the Policy Author to provide details on the policy, procedure, practice and/or decision being screened and what available evidence you have gathered to help make an assessment of the likely impact on equality of opportunity and good relations. Reference to policy within this document refers to either of the aforementioned (policy, procedure, practice, and/ or decision).

Section 2 – Screening questions

This asks about the extent of the likely impact of the policy on groups of people within each of the Section 75 categories. Details of the groups consulted and the level of assessment of the likely impact. This includes consideration of multiple identity and issues.

Section 3 –Screening decision

This guides the Council to reach a screening decision as to whether or not there is a need to carry out an equality impact assessment (EQIA), or introduce measures to mitigate the likely impact, or the introduction of an alternative policy to better promote equality of opportunity.

Section 4 – Monitoring

This provides guidance to the Council on monitoring for adverse impact and broader monitoring.

Section 5 – Approval and authorisation

This verifies the Council's approval of a screening decision by a senior manager responsible for the policy.

Appendix A Screening Process

Section 1 Policy Scoping & Information

The first stage of the screening process involves scoping the policy under consideration which sets the context and confirms the aims and objectives for the policy being screened. Scoping the policy helps to identify constraints as well as opportunities and will help the policy author to work through the screening process on a step by step basis.

1. Policy Name		
Data Protection Policy		
2. Is this an existing, revised or a new policy?		
Revised Policy		
3. What is it trying to achieve? (aims/outcomes)		
This practice has been revised to reflect current practice and guidance.		
4. Are there any Section 75 categories which might be expected to benefit from the intended policy?	Yes	
	No	X
If so, please explain		
5. Who initiated or wrote the policy?		
Mid Ulster District Council		
6. Who owns and who implements the policy?		
Mid Ulster District Council		

Implementation factors

		Yes	No
Are there any factors which could contribute to/ detract from intended aim/ outcome of the policy?			
• If yes, are they financial?			X
• If yes, are they legislative?		X	
• If yes, Please specify	***Legislative*** Data Protection Act 2018		
• Other, Please specify			

Stakeholders

The internal and external (actual or potential) that the policy will be impacted upon

	Yes	No
Staff	X	
Service Users	X	
Other public sector organisations	X	
Voluntary/community/ trade unions	X	
Other, please specify	Councillors, Contractors	

Others policies with a bearing on this policy

Policies	Owners
All HR & ICT Policies	Organisational Development

Available evidence

Information and available evidence (qualitative and quantitative) gathered to inform the policy under each of the Section 75 groups as identified within the Northern Ireland Act 1998. [Add information and evidence from other sources, eg, research, survey findings, service user feedback, consultation feedback, review findings, etc]

Section 75 category	Details of evidence/information
Religious belief	**Data not currently available**
Political opinion	**The political opinion of the staff of Mid Ulster District Council can currently be broken down as follows:** **Generally Nationalist- 7%** **Generally Unionist- 3%** **Neither Generally Unionist or Nationalist-3%** **Unknown- 87%**
Racial group	**The racial grouping of the staff of Mid Ulster District Council can currently be broken down as follows:** **White- 92.6%** **Mixed Ethnic- 0.8%** **Black/Caribbean/Other 0.3%** **Unknown- 5.3%**
Age	**The age of the staff of Mid Ulster District Council can currently be broken down as follows:** **17-25yrs- 16.4%** **26-35yrs- 16.3%** **36-45yrs- 23.3%** **46-55yrs 23.3%** **56-65yrs 16.3%** **66-75yrs- 3%** **Unknown- 0.8%**

Marital status	**The marital status of the staff of Mid Ulster District Council can currently be broken down as follows:** **Married 55%** **Single 39%** **Unknow 3%** **Divorced/Separated/Widowed 3%**
Sexual orientation	**The sexual orientation of the staff of Mid Ulster District Council can currently be broken down as follows:** **Heterosexual- 13%** **Did not want to disclose- 0.6%** **Unknown- 86.3%** **Lesbian- 0.09%**
Men & women generally	**The gender breakdown of the staff of Mid Ulster District Council can currently be broken down as follows:** **58% are men** **42% are women**
Disability	**Currently 2% of Mid Ulster District Council staff have stated that they have a disability.**
Dependants	**The breakdown of the Mid Ulster District Council staff who have dependents can currently be broken down as follows:** **No Dependents- 9%** **Carer for an Adult- 0.5%** **Child/Children- 4.5%** **Unknown- 86%**

Needs, experiences and priorities

Taking into account the information referred to above, what are the different needs, experiences and priorities of each of the following categories, in relation to the particular policy/decision? Specify details for each of the Section 75 categories

Section 75 category	**Details of needs/experiences/priorities**
Religious belief	**Data not currently available**
Political opinion	**The political opinion of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **Generally Nationalist- 10%** **Generally Unionist- 3%** **Neither Generally Unionist or Nationalist-2%** **Unknown- 85%**
Racial group	**The racial grouping of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **White- 89%** **Mixed Ethnic- 1%** **Unknown- 10%**
Age	**The age categories of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **17-25yrs- 27%** **26-35yrs- 20%** **36-45yrs- 15%** **46-55yrs 15%** **56-65yrs 16%** **66-75yrs- 6%**

	Unknown- 1%
Marital status	**The martial status of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **Married 41%** **Single 53%** **Unknow 4%** **Divorced/Separated/Widowed 3%**
Sexual orientation	**The sexual orientation of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **Heterosexual- 17%** **Did not want to disclose- 1%** **Unknown- 82%**
Men and women generally	**The gender of the staff of Mid Ulster District Council who have been entered into the Jobs Retention Scheme can currently be broken down as follows:** **Men- 53%** **Women- 47%**
Disability	**0%**
Dependants	**The breakdown of the Mid Ulster District Council staff who have dependents can currently be broken down as follows:** **No Dependents- 13%** **Child/Children- 4%** **Unknown- 83%**

Section 2 – Screening Questions

In making a decision as to carry out an Equality Impact Assessment (EQIA), the Council should consider its answers to the questions 1- 3 detailed below.

If the Council's conclusion is **none** in respect of all of the Section 75 equality of opportunity categories, then the Council may decide to screen the policy out. If a policy is 'screened out' as having no relevance to equality of opportunity, the Council should give details of the reasons for the decision taken.

If the Council's conclusion is **major** in respect of one or more of the Section 75 equality of opportunity, then consideration should be given to subjecting the policy to the equality impact assessment procedure.

If the Council's conclusion is **minor** in respect of one or more of the Section 75 equality categories, then consideration should still be given to proceeding with an equality impact assessment, or to:

- measures to mitigate the adverse impact; or
- the introduction of an alternative policy to better promote equality of opportunity.

In favour of a 'major' impact

a) The policy is significant in terms of its strategic importance;

b) Potential equality impacts are unknown, because, for example, there is insufficient data upon which to make an assessment or because they are complex, and it would be appropriate to conduct an equality impact assessment in order to better assess them;

c) Potential equality impacts are likely to be adverse or are likely to be experienced disproportionately by groups of people including those who are marginalised or disadvantaged;

d) Further assessment offers a valuable way to examine the evidence and develop recommendations in respect of a policy about which there are concerns amongst affected individuals and representative groups, for example in respect of multiple identities;

e) The policy is likely to be challenged by way of judicial review;

f) The policy is significant in terms of expenditure.

In favour of 'minor' impact

a) The policy is not unlawfully discriminatory and any residual potential impacts on people are judged to be negligible;

b) The policy, or certain proposals within it, are potentially unlawfully discriminatory, but this possibility can readily and easily be eliminated by making appropriate changes to the policy or by adopting appropriate mitigating measures;

c) Any asymmetrical equality impacts caused by the policy are intentional because they are specifically designed to promote equality of opportunity for particular groups of disadvantaged people;

d) By amending the policy there are better opportunities to better promote equality of opportunity.

In favour of none

a) The policy has no relevance to equality of opportunity.

b) The policy is purely technical in nature and will have no bearing in terms of its likely impact on equality of opportunity for people within the equality categories.

Screening questions

1. What is the likely impact on equality of opportunity for those affected by this policy, for each of the Section 75 equality categories (minor/ major/ none)		
Section 75 category	Details of policy impact	Level of impact? minor/major/none
Religious belief	No adverse impacts anticipated	None
Political opinion	No adverse impacts anticipated	None
Racial group	No adverse impacts anticipated	None
Age	No adverse impacts anticipated	None
Marital status	No adverse impacts anticipated	None
Sexual orientation	No adverse impacts anticipated	None

Men and women generally	No adverse impacts anticipated	None
Disability	No adverse impacts anticipated	None
Dependants	No adverse impacts anticipated	None

2. Are there opportunities to better promote equality of opportunity for people within Section 75 equality categories? (Yes/ No)		
Section 75 category	If **Yes,** provide details	If **No,** provide reasons
Religious belief		This is an internal ICT policy with no opportunity to better promote equality issues.
Political opinion		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Racial group		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Age		Mid Ulster District Council has assessed the potential impact

		of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Marital status		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Sexual orientation		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Men and women generally		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Disability		Mid Ulster District Council has assessed the potential impact of the policy . Council has determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.
Dependants		Mid Ulster District Council has assessed the potential impact of the policy . Council has

		determined it does not unlawfully directly discriminate in any way with respect to any Section 75 groups.

3. Are there opportunities without prejudice, to the equality of opportunity duty, to better promote good relations between Section 75 equality categories, through tackling prejudice and/ or promoting understanding? (Yes/ No)		
	No	x
	Yes	
If yes, please detail the opportunities below:		

If yes is concluded to Question 3, then the policy will be referred to the Council's Good Relations Working Group for consideration. The Group will consider the potential opportunities and assess if and how the overall impact of a decision/policy can better promote good relations.

Additional Considerations - Multiple identity

Generally speaking, people can fall into more than one Section 75 category. Taking this into consideration, are there any potential impacts of the policy/decision on people with multiple identities? (*For example; disabled minority ethnic people; disabled women; young Protestant men; and young lesbians, gay and bisexual people).*
Mid Ulster District Council considers that there are no potential impacts for those with multiple identities under S75 by revising this policy.
Provide details of data on the impact of the policy on people with multiple identities. Specify relevant Section 75 categories concerned.

Section 3 – Screening Decision

In light of answers provided to the questions within Section 3 select one of the following with regards the policy:

		Select One
1	Shall not be subject to an EQIA - *with no mitigating measures required*	X
2	Shall not be subject to an EQIA - *mitigating measures/ alternative policies introduced*	
3	Shall be subject to an EQIA	

If 1 or 2 above (i.e. not to be subject to an EQIA) please provide details of reasons why.
N/A

If 2 above (i.e. not to subject to an EQIA) in what ways can adverse impacts attaching to the policy be mitigated or an alternative policy be introduced.
N/A

If 3 above (i.e. shall be subject to an EQIA), please provide details of the reasons.
N/A

Mitigation

When it is concluded that the likely impact is ‘minor’ and an equality impact assessment is not to be conducted, you may consider mitigation to lessen the severity of any equality impact, or the introduction of an alternative policy to better promote equality of opportunity.

Can the policy/decision be amended or changed or an alternative policy introduced to better promote equality of opportunity?
If so, give the **reasons** to support your decision, together with the proposed changes/amendments or alternative policy: It has not been identified that mitigation is required in relation to this policy.

Timetabling and prioritising

If the policy has been screened in for equality impact assessment, please answer the below to determine its priority for timetabling the equality impact assessment.

- **On a scale of 1-3 (1 being lowest priority and 3 being highest), assess the policy in terms of its priority for equality impact assessment**.

Priority criterion	**Rating (1-3)**
Effect on equality of opportunity	
Social need	
Effect on people's daily lives	
Relevance to a Council's functions	

Note: The Total Rating Score should be used to prioritise the policy in rank order with other policies screened in for equality impact assessment. This list of priorities will assist the Council in timetabling. Details of the Council's Equality Impact Assessment Timetable should be included in the Screening Reports.

- **Is the policy affected by timetables established by other relevant public authorities?**

Yes	
No	X

Section 5 – Monitoring

Effective monitoring will help identify any future adverse impact arising from the policy which may lead the Council to conduct an equality impact assessment, as well as help with future planning and policy development. Please detail proposed monitoring arrangements below:

The implementation of this practice will be monitored against the timeframe of Council being able to reopen all areas of service delivery. The Jobs Retention Scheme will be in place until 31st October 2020. Any further action in relation to the implementation of the Scheme will require further screening at that point.

Section 6 – Approval and authorisation

Screened by:	**Position/ Job Title**	**Date**
Ann McAleer	Corporate Policy & Equality Officer	
Approved by: (Director)	**Position/ Job Title**	**Date**

Note: A copy of the Screening Template, for each policy screened should be 'signed off' and approved by a senior manager responsible for the policy; made easily accessible on the council website as soon as possible following completion and be available on request.

Appendix A **Mid Ulster District Council Screening Process**