Data Protection Policy

January 2019

ARMAGH CITY, BANBRIDGE AND CRAIGAVON BOROUGH COUNCIL	
Document Reference Number:	**GPRC/P21/V2.0**
Title of Policy:	**Data Protection Policy**
No of Pages (including appendices):	**32**
Version:	**V2.0**
Issue Date:	
Policy Nominated Officer:	**Joan Farley, Senior Records Manager**
Equality screened/Rural Impact Assessed by	**Joan Farley, Senior Records Manager**
Equality screening/Rural Impact Assessment date:	**10 January 2019**
Amendment Version Issue Date:	**10 January 2019**
Sent out by:	**Eamonn Kelly, Head of Governance & Democratic Services**
Approved by:	
Review Date:	**January 2022**

AMENDMENT RECORD SHEET

Remove and destroy old pages. Insert new pages as indicated.

Revision Number	Page Number	Date Revised	Description of Revision
SGC/P5.0/V1.0			Aligned to DPA2018 & GDPR

CONTENTS

1. INTRODUCTION

1.1. Armagh City, Banbridge and Craigavon Borough Council needs to collect personal information about citizens with whom it deals with in order to carry out its business and provide services. This includes citizens, employees (past, present and prospective), suppliers and other business contacts. In addition, we may be required by law to process and share personal information with other organisations (including, but not limited to, PSNI and regulatory bodies).

1.2. As a public body, Council has a statutory duty to safeguard the information it holds, from whatever source, which is not in the public domain. The lawful and proper treatment of personal information by Council is extremely important to the success of our organisation and in order to maintain the confidence of our service users and employees.

2. THE DATA PROTECTION PRINCIPLES

2.1 Council, its staff and others who process personal information on its behalf must ensure that they follow the principles set out within Article 5 of the General Data Protection Regulation (GDPR), namely that personal information will be:

(a) processed lawfully, fairly and in a transparent manner;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(d) accurate and, where necessary, kept up to date;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. SUPPORTING LEGISLATION

3.1 The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies in the UK. There are three separate regimes set out in the DPA 2018 and our processing falls under the general processing regime which is Part 2 of the DPA 2018.

As well as ensuring compliance with DPA 2018 Council must also adhere to the legal requirements and best practice guidance, which includes but is not limited to:

- General Data Protection Regulation (EU)2016/679
- Common Law duty of confidentiality
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Access to Health Records (Northern Ireland) Order 1993
- Human Rights Act 1998

- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioner's Office
- Council's Retention and Disposal schedule

4. NOTIFICATION

4.1 Under the 2018 Regulations, Armagh City, Banbridge and Craigavon Borough Council, as data controller must pay a data protection fee. The new data protection fee replaces the requirement to 'notify' (or register), which was in the Data Protection Act 1998. The fee is set by Parliament and reflects what Parliament feels is appropriate, based on the risks that the processing of personal data presents. Council are eligible to pay a fee in tier 3.

5. PURPOSE

5.1 The purpose of this policy is to lay down the principles that must be observed by anyone who works for, or on behalf of, Council and has access to personal information.

5.2 This policy aims to clarify how and when personal information may be shared, and the need to make individuals aware of the ways in which their information might be used.

6. SCOPE

6.1 The scope of this policy is to support the protection, control and management of personal information. The policy will cover all information within Council and is concerned with all information systems, electronic and non-electronic information. It applies to all directorates, services and departments, all permanent and temporary staff, all agency workers, and as appropriate to contractors and third party service providers acting on behalf of Council.

6.2 This includes, but is not necessarily limited to information:

- stored on computers, paper and electronic structured/unstructured records systems;
- transmitted across internal and public networks such as email or intranet/internet;
- stored within databases;
- printed or handwritten;
- stored on removable media such as cds, hard disks, pen drives, tapes and other similar media;
- stored on fixed media such as hard drives and disk subsystems;
- held on film or microfiche;
- information recording and processing systems whether paper, electronic, video, CCTV, or audio records;
- presented on slides, overhead projectors, using visual and audio media;
- spoken during telephone calls and meetings or conveyed by any other method.

6.3 This policy covers all forms of information held, including (but not limited to):

- information about members of the public; non-employees on organisational premises;
- staff and personal information;
- organisational, business and operational information.

6.4 This policy covers all information systems purchased, developed and managed by/or on behalf of, Council and any individual directly employed or otherwise used by Council.

7. DEFINITIONS

7.1 **Personal Data**

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.

Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.

Information about companies or public authorities is not personal data.

However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

7.2 **Special categories of personal information**

Special category data is more sensitive, and so needs more protection. Article 9 of GDPR defines 'special categories' of personal information as information relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);

- health;
- sex life; or
- sexual orientation.

7.3 **Data Controller**

A controller determines the purposes and means of processing personal data.

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

Controllers shoulder the highest level of compliance responsibility – you must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. You are also responsible for the compliance of your processor(s).

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.

7.4 **Data Processor**

A processor is responsible for processing personal data on behalf of a controller.

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

Processors do not have the same obligations as controllers under the GDPR and do not have to pay a data protection fee. However, if you are a processor, you do have a number of direct obligations of your own under the GDPR.

Both supervisory authorities (such as the ICO) and individuals may take action against a processor regarding a breach of those obligations.

8. OBJECTIVES

8.1 Council will apply the above principles to the management of all personal information by adopting the following policy objectives:

8.1.1 **Privacy by Design**

Council will apply 'privacy by design' when developing and managing information systems containing personal information by:

- Using proportionate Data Protection Impact Assessment (DPIA) to identify and mitigate data protection risks at an early stage of project and process design for all new or updated systems and processes;
- Adopting data minimisation: Council will collect, disclose and retain the minimum personal information for the minimum time necessary for the purpose(s) that it is being processed; and
- Anonymising personal information wherever necessary and appropriate, for instance when using it for statistical purposes.

For further information, please refer to Council's Data Protection Impact Assessment protocol (Appendix A).

8.1.2 **Fair and Lawful Processing**

Council will only collect and use personal information to the extent that it is needed to fulfil operational or legal requirements, and in accordance with the conditions set down under GDPR, namely:

- Consent of the data subject;
- To perform in terms of a contract;
- To comply with a legal obligation;
- To protect a data subject's vital interests;
- If it is in the public interest.

Council will provide transparent information on how personal information will be processed by way of 'fair processing notice', which will detail:

- What information is needed;
- Why this information is needed;
- The purpose(s) that this information will be used for;
- How long this information will be kept for;
- Ensure that personal information is collected for specific purpose(s), and will not be reused for a different purpose that the individual did not agree to or expect;
- Ensure the quality of personal information processed.

8.1.3 **Disclosure of Personal Information**

Strict conditions apply to the disclosure of personal information both internally and externally. Council will not disclose personal information to any third party unless it is lawful to do so. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the individual has consented to the disclosure; or
- the information is in a form that does not identify the individual.

8.1.4 **Right of Access**

GDPR gives any individual who has personal information kept about them by Council the right to request in writing a copy of the information held relating to them. Council will ensure that an applicant receives access within a calendar month, unless there is a valid reason for delay or an exemption is applicable.

A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for his or her own personal data.

This presents a challenge as any member of staff could receive a subject access

request. However, Council have a legal responsibility to identify that an individual has made a request and to handle it accordingly.

For further information, please refer to Council's Access to Information Policy – Section 8.
https://www.armaghbanbridgecraigavon.gov.uk/download/51/policies/25443/access-to-information-policy.pdf

8.1.5 **Safeguarding Information**

Council will ensure appropriate technical and organisational security measures are in place to safeguard personal information so as to prevent loss, destruction or unauthorised disclosure.

8.1.6 **Retention and Disposal**

GDPR places an obligation on Council not to keep personal information for longer than is required for the purpose(s) for which it was collected. Personal information will be disposed of by means that protect the rights of those individuals, and as such Council will:

- Apply retention policies to all personal information;
- Destroy information no longer required in a secure manner; or
- Transfer the information, by arrangement, to the Public Records Office of Northern Ireland (PRONI) where deemed appropriate.

8.1.7 **Uphold Individual's Rights**

Council will ensure that the rights of the individual under GDPR are upheld, where applicable, namely:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- The rights in relation to automated decision making and profiling.

9. RESPONSIBILITY

9.1 The Executive Management Team (EMT) will have overall responsibility for the implementation of Council's Data Protection Policy. Each Strategic Director will assume responsibility for the compliance of staff within their department.

9.2 The Chief Executive has ultimate responsibility for the delivery of this policy and subsequent policies and procedures.

9.3 The Strategic Director (Performance) will assume responsibility as Senior Information Risk Officer (SIRO) to ensure compliance with legislation through the development and monitoring of policy and codes of practice.

9.4 The Data Protection Officer (DPO) will provide advice and guidance on data protection

and implementation to ensure compliance with the GDPR requirements.

9.5 Managers are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes.

9.6 All staff members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff are expected to:

- Familiarise themselves with, and abide by, the principles set out within this policy;
- Understand how to safeguard personal information.
- Any third parties who are users of personal information processed by Council will be required to confirm and demonstrate that they will abide by the requirements of GDPR.

10. NON-COMPLIANCE

A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and/or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. In relation to the use of ICT equipment including the use of the internet and email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

All data breach incidents will be handled in accordance with the Data Breach Incident Handling Protocol (see Appendix B).

Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

11. PERFORMANCE AND MONITORING COMPLIANCE

The effectiveness of this policy will be assessed on a number of factors:

- nomination of a Data Protection Officer (DPO) with specific responsibility for data protection within Council;
- compliance with legislation in respect of GDPR;
- the management of data breaches, including near misses;
- the retention and disposal of records in accordance with Council's Retention & Disposal Schedule.

The DPO will maintain a central record of all breaches in line with Article 33(5).

12. ASSOCIATED GUIDANCE DOCUMENTS

- Data Protection Impact Assessment Protocol (Appendix A)
- Data Breach Incident Handling Protocol (Appendix B)
- Flowchart showing Notification Requirements (Appendix C)

- Examples of what constitutes a personal data breach and who to notify (Appendix D)

13. REVIEW

This policy and associated documents will be reviewed regularly and all employees advised of any amendments/updates.

The policy will also be reviewed in the event of:

- changes in legislative requirements;
- changes in Government directives or Codes of Practice;
- changes in Council policy.

Appendix A - Data Protection Impact Assessment Protocol and Associated Documents

Contents

Introduction

This protocol has been developed to ensure that Council can meet its requirements for Data Protection Impact Assessments (DPIAs) under the General Data Protection Regulation (GDPR) and to ensure we embed them into our normal business practices.

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project or plan. This is a key part of the Council's accountability obligations under the GDPR as well as a key element of data protection by design and by default, and also reflects the more risk-based approach to data protection obligations taken throughout the GDPR.

It is important to bear in mind that DPIAs are also relevant if you are planning to make changes to an existing system. In this case, you must ensure that you do the DPIA at a point when there is a realistic opportunity to influence those plans.

You may use a DPIA to review your existing processing operations, to identify whether you already do anything that would be considered likely high risk under the GDPR.

- If so, are you confident that you have already adequately assessed and mitigated the risks of that project?
- If not, you may need to conduct a DPIA now to ensure the processing complies with the GDPR.

In line with Information Commissioner's Office (ICO) guidance, Council does not expect you to complete a new DPIA for established processing where you have already considered relevant risks and safeguards (whether as part of a Privacy Impact Assessment (PIA) or another formal or informal risk assessment process) - unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.

What is a DPIA?

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm –- to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It is important to embed DPIAs into Council processes and ensure the outcome can influence our plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it.

DPIAs are mandatory for any **processing** that is **likely to result in a high risk** to individuals. Failing to carry out a DPIA in these cases may leave you open to enforcement action from the ICO, including a fine.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

DPIAs are not just a compliance exercise. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and your organisation.

A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you have put in place on an ongoing basis. You need to keep it under review and reassess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your DPIA assesses any new risks. An external change to the wider context of the processing should also prompt you to review your DPIA, for example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects.

What kind of 'risk' do they assess?

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The key provision here is Recital 75, which links risk to the concept of potential harm or damage to individuals. The focus is therefore on any potential harm to individuals.

However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage".
The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if your intended processing leads to a loss of public trust.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

Remember: *If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.* (Note: If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.)

The following associated documents have been included to assist you:

Appendix 1 DPIA decision flowchart and life cycle – The flowchart gives you a high-level graphical overview of the process.

Appendix 2 DPIA screening checklist – This should be used so that you can determining if you need to conduct a DPIA

Appendix 3 DPIA template – The template should be completed to ensure you follow the DPIA process.

How do we conclude our DPIA?

What happens next?
You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to consult the ICO before you can go ahead with the processing.

It is good practice to publish your DPIA to aid transparency and accountability. This could help foster trust in your processing activities, and improve individuals' ability to exercise their rights.

If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary. Council may need to consider its freedom of information obligations.

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

If you want your project to proceed effectively then investing time in producing a comprehensive DPIA may prevent any delays later.

When do we need to consult the ICO?

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so.

The DPO will complete the ICO online form and submit a copy of your DPIA.

ICO will conduct a brief screening exercise to check that your DPIA does identify a high risk that has not been mitigated. If there is no residual high risk, the ICO will let you know that they don't need to review the DPIA.

The ICO will notified the DPO if your DPIA has been accepted for consultation (usually within ten days of sending it to the ICO).

What are the possible outcomes?

ICO will provide a written response, advising that:

- the risks are acceptable and you can go ahead with the processing;

- you need to take further measures to reduce the risks;
- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

How long does it take?

In most cases the ICO will get back to us within eight weeks. In complex cases they may extend this to a maximum of 14 weeks. If the ICO need to extend the deadline, they will let us know within one month of the date of submission of your DPIA and they will explain their reasons.

If the ICO needs to ask for additional information, the clock will stop until you provide the requested details.

In some cases, the ICO may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

Can we appeal?

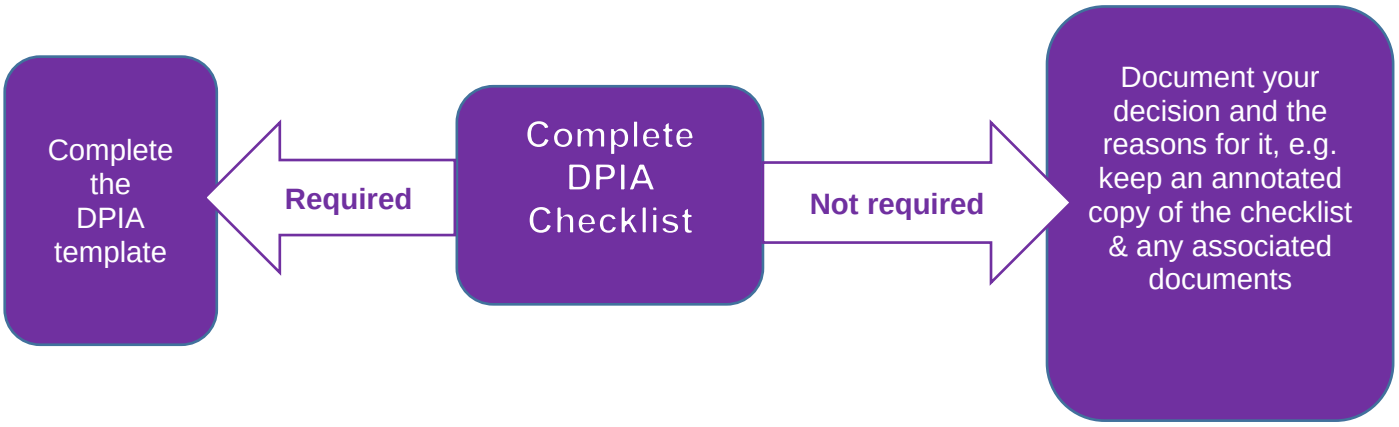
Requests for review/appeal need to be sent to the ICO via the DPO. The DPO will provide advice on the process.

There are two stages to the review/appeal process. In the first instance, if Council disagree with the ICO advice, we can ask them to review their decision.

If Council are not happy with the outcome of the review, in certain cases, we can appeal to the First Tier Tribunal.

Appendix 1 - DPIA Decision Flowchart and Life Cycle

DPIA Decision Flow Chart



DPIA Life Cycle

Appendix 2 - DPIA Screening Checklist

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk".

This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

Council in line with GDPR will conduct a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.

Council in line with the ICO guidance will conduct a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

Council will consider whether to do a DPIA if we plan to carry out any other:

- Processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.
- If there is a change to the nature, scope, context or purposes of our processing.

If we decide not to carry out a DPIA, we document our reasons.

E.g. keep an annotated copy of the checklist and any associated documents.

If we decide to carry out a DPIA, we will use the DPIA template in Appendix 3 and follow the approval process contain within the template.

Appendix 3 - DPIA Template

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves (you may find it helpful to refer or link to other documents, such as a project proposal). Include a summary detailing why you identified the need for a DPIA.
If you have any major project which involves the use of personal data it is good practice to carry out a DPIA. If you already intend to do a DPIA, go straight to step 2. *Otherwise, you need to check whether your processing is on the list of types of processing which automatically require a DPIA. If not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.* *You can use or adapt the checklists at contained in this protocol to help you carry out this screening exercise. You can also read further guidance on the ICO website 'When do we need to do a DPIA?'* *If you carry out this screening exercise and decide that you **do not** need to do a DPIA, you should document your decision and the reasons for it, including your DPO's advice. This does not have to be an onerous paperwork exercise – as long as it helps you demonstrate that you have properly considered and complied with your DPIA obligations. For example, you could simply keep an annotated copy of the checklist* *If you are in any doubt, we strongly recommend you do a DPIA.*

Step 2: Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? (you might find it useful to refer to a flow diagram or other way of describing data flows). What types of processing identified as likely high risk are involved?

Describe how and why you plan to use the personal data. Your description must include "the nature, scope, context and purposes of the processing".

The nature of the processing is what you plan to do with the personal data. This should include, for example:

- *how you collect the data;*
- *how you store the data;*
- *how you use the data;*
- *who has access to the data;*
- *who you share the data with;*
- *whether you use any processors;*
- *retention periods;*
- *security measures;*
- *whether you are using any new technologies;*
- *whether you are using any novel types of processing; and*
- *which screening criteria you flagged as likely high risk.*

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe:

- *the nature of the personal data;*
- *the volume and variety of the personal data;*
- *the sensitivity of the personal data;*
- *the extent and frequency of the processing;*
- *the duration of the processing;*
- *the number of data subjects involved; and*
- *the geographical area covered.*

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe: • *the source of the data;* • *the nature of your relationship with the individuals;* • *the extent to which individuals have control over their data;* • *the extent to which individuals are likely to expect the processing;* • *whether they include children or other vulnerable people;* • *any previous experience of this type of processing;* • *any relevant advances in technology or security;* • *any current issues of public concern; and* • *in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes.* • *whether you have considered and complied with relevant codes of practice.*

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Describe: • *your legitimate interests, where relevant;* • *the intended outcome for individuals; and* • *the expected benefits for you or for society as a whole.*

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within Council? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
You should seek the views of individuals (or their representatives) unless there is a good reason not to. *In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of your DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.* *If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.* *If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.* *If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.* *If you use a data processor, you may need to ask them for information and assistance. Your contracts with processors should require them to assist.* *You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.* *ICO also recommend you consider seeking legal advice or advice from other independent experts such as IT experts, sociologists or ethicists where appropriate. However, there are no specific requirements to do so.* *In some circumstances you might also need to consult the ICO once you have completed your DPIA. See the next section of this guidance for more information.*

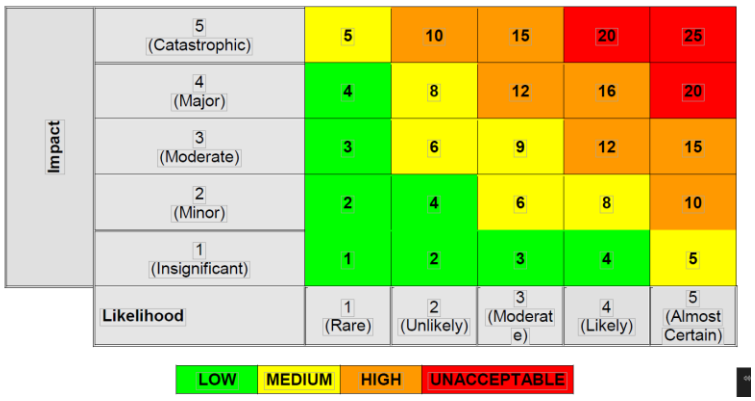
Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Do your plans help to achieve your purpose? *Is there any other reasonable way to achieve the same result?* *Describe:* • *your lawful basis for the processing;* • *how you will prevent function creep;* • *how you intend to ensure data quality;* • *how you intend to ensure data minimisation;* • *how you intend to provide privacy information to individuals;* • *how you implement and support individuals rights;* • *measures to ensure your processors comply; and* • *safeguards for international transfers.*

Step 5: Identify and Assess Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to: • *inability to exercise rights (including but not limited to privacy rights);* • *inability to access services or opportunities;* • *loss of control over the use of personal data;* • *discrimination;* • *identity theft or fraud;* • *financial loss;* • *reputational damage;* • *physical harm;* • *loss of confidentiality;* • *reidentification of pseudonymised data; or* • *any other significant economic or social disadvantage* *You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).* *To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.* *You must make an 'objective assessment' of the risks. You might find it helpful to use a structured matrix to think about*	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

likelihood and severity of risks:



Please refer to ***Corporate Risk Management Policy***

(insert hyperlink here…)

You might also want to consider your own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

Step 6: Identify Measures to Reduce Risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
	Against each risk identified, record the source of that risk. You should then consider options for reducing that risk. For example: • *deciding not to collect certain types of data;* • *reducing the scope of the processing;* • *reducing retention periods;* • *taking additional technological security measures;* • *training staff to ensure risks are anticipated and managed;* • *anonymising or pseudonymising data where possible;* • *writing internal guidance or processes to avoid risks;* • *adding a human element to review automated decisions;* • *using a different technology;* • *putting clear data sharing agreements into place;* • *making changes to privacy notices;* • *offering individuals the chance to opt out where appropriate; or* • *implementing new systems to help individuals to exercise their rights.* *This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask your DPO for advice.* *Record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.*	Eliminated reduced accepted	Low/Medium /High	Yes/No

Step 7: Sign-Off and Record of Outcomes

	Name/Date	**Notes**
Measures approved by:		*What additional measures you plan to take.* *Whether each risk has been eliminated, reduced, or accepted;* *How will you integrate actions back into project plan, with date and responsibility for completion?*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice: *As part of the sign-off process, you should ask your DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.*		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:		*The reviewing officer should advise the DPO of any changes to ensure ongoing compliance.*

Appendix B - Data Breach Incident Handling Protocol

Introduction

Council has a responsibility to monitor all incidents that occur within the organisation that may breach security and/or confidentiality of information. All incidents need to be identified, reported, investigated and monitored. If the breach is likely to result in a risk to individuals' rights and freedoms appropriate action must be taken. It is only by adopting this approach that Council can prevent reoccurrence of such incidents.

It is important that Council and its staff learn from reported incidents. "Near misses" will also be reported and investigated to ensure that lessons can be learned and procedures improved.

Types of Data Breach Incidents

Breaches of information security and/or confidentiality could potentially compromise business operations and be damaging to Council as a whole. Such breaches could result in a high risk to individuals' rights and freedoms and may lead to disciplinary action and possibly legal sanctions.

Examples of these types of incident include:

- Damage to or theft/loss of information (either manual or electronic)
- Leaving confidential information/records in a public area
- Incorrect disposal of confidential waste
- Unauthorised access to information
- Unauthorised disclosure of confidential information in any format including verbally
- Transfer of information to the wrong person (by email, fax, post or phone)
- Sharing of computer IDs and passwords.

Every breach must be taken seriously and reported according to the process identified in this document. If there is any doubt about what constitutes a security incident, staff should contact the ICT department.

Reporting of Incidents

Staff will be made aware that any incident or suspected incident must be reported immediately to their line manager as a data breach.

Incident Investigation, Recording and Follow-up

When an incident is detected it should be reported to the line manager/ senior officer. The manager/ senior officer will advise the appropriate Head of Department and agree who should make an initial assessment (the nominated officer). This will determine the significance of the data breach and whether further action and/or investigation is warranted. This will include assessment of the type of data involved and risks associated with its loss.

The nominated officer will discuss the incident with the Data Protection Officer (DPO) to establish notification requirements and action for containment. The DPO will advise on notification requirements.

The nominated officer will complete the Data Breach Incident Reporting Template (see below) and send it to dataprotection@armaghbanbridgecraigavon.gov.uk so that the DPO can maintain a central record of all Breaches in line with Article 33(5) of GDPR. Significant incidents will be reported to the (appropriate) Committee.

Where appropriate, it may be necessary to conduct an investigation to establish the circumstances of the incident, the extent of any loss and the implications for Council.

The investigation will consider:

- Details of the data breach
- Type of data placed at risk
- Containment and recovery
- Lessons learnt
- Training and guidance
- Evaluation

Data Breach Incident Reporting Template (and Guidance Notes)

Details of the data breach:

Please describe the incident in as much detail as possible, including:

- *When did the incident happen?*
- *How did the incident happen?*
- *If there has been a delay in reporting the incident, please explain your reasons for this.*
- *What measures have been put in place to prevent an incident of this nature occurring?*
- *Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.*

Type of data placed at risk:

Assess the type of data and any risks associated with the breach:

- *Is this a personal data breach? A 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. This includes breaches that are the result of both accidental and deliberate causes.*
- *Are the associated risks likely to affect what you do once the breach has been contained (in particular, assess the potential risk to individuals' rights and freedoms and or the organisation).*

  Note: GDPR makes clear that a risk to individuals' rights and freedoms is about the potential for any type of impact. This includes physical, financial or any other impact, such as:
  - *inability to exercise rights (including data protection rights);*
  - *loss of control over the use of personal data; or*
  - *any social or economic disadvantage.*

  - *Are the associated risks likely to affect what you do once the breach has been contained (in particular, assess the potential risk to individuals' rights and freedoms and or the organisation).*

Containment and recovery:

Detail any recovery plan and, where necessary, procedures for damage limitation:

- *Detail of recovery plan (where necessary)? GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it*

- *Do you need to inform those affected? (One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach).*

- *If you decide not to notify individual, you may still need to notify the ICO unless you can demonstrate that the breach in unlikely to result in a risk to the rights and freedoms. You must document your decision making process in line with the requirements of accountability.*

- *Is there a requirement to notify the ICO, PSNI or other regulatory body?*

Training and guidance:

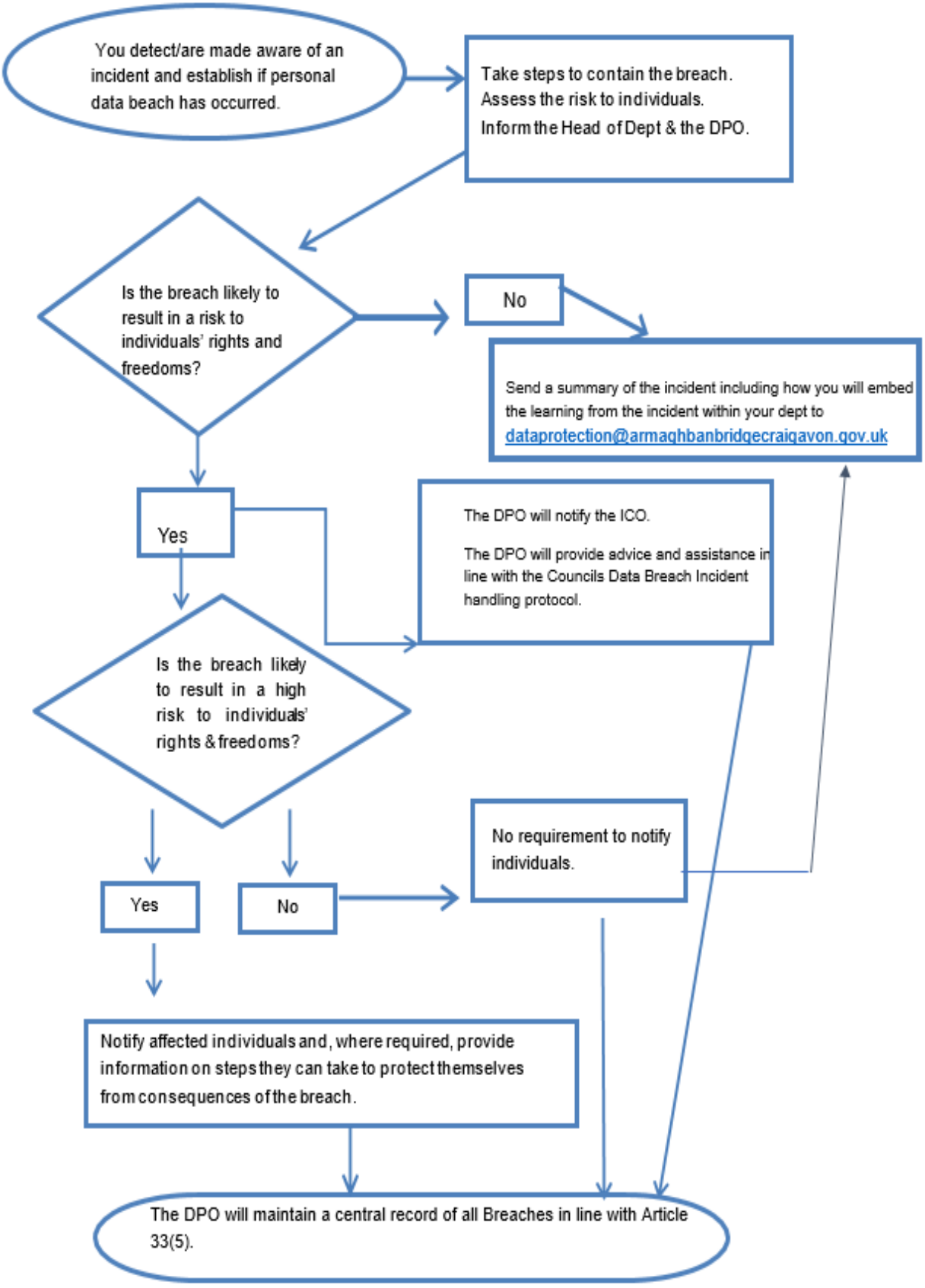
Please provide details of relevant training Council has provided to staff? and provide any extracts relevant to this incident here:

- *Please include details of any guidance issued to staff on the handling of data in relation to the incident you are reporting? (Provide any extracts relevant to this incident here).*

Record of Reporting:		
	Date:	**Name:**
Reporting Officer:		
Nominated Officer:		
Head of Department notified:		
DPO advice provided:		

Record of Outcomes:	
Summary of DPO advice:	
Summary of Actions taken:	
Details of Actions to be taken:	
Details of Reporting:	e.g. reported to the (appropriate) committee.

Appendix C - Flowchart showing Notification Requirements



Appendix D - Examples of Personal Data Breaches and Who to Notify

The following non-exhaustive examples will assist staff in determining appropriate actions and the type of incident that requires notification to the ICO in different personal data breach scenarios. These examples may also help staff to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/ recommendations
A stored backup of an archive of personal data is held on encrypted on a USB key. The key is stolen or lost.	No.	No.	As the data is encrypted and a backup of the data exists, the data is not compromised, and the data can be restored, this may not be a reportable breach. However if it is later compromised, notification would be required.
Council maintains an online service. As a result of a cyber-attack on that service, personal data of individuals are exfiltrated.	Yes, report to the ICO if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
A brief power outage lasting several minutes at means that the public are unable to call the Council and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
Council suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality	Yes, report to the ICO, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the ICO

was to encrypt the data, and that there was no other malware present in the system.			became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
An individual phones a Council to report a data breach. The individual has received information for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes, report to the ICO.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the Council should take the additional step of notifying other individuals if there is high risk to them.
A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the law means that any user can access the details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider. If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have but it is likely to be recordable or be a matter of non-compliance under Article 32.

	aware" once they have been notified by the hosting company (the processor). The controller then must notify the ICO.		
Personal data of a large number of citizens are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to ICO.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Appendix E - Policy Screening Form

Policy Scoping

Policy Title: Data Protection Policy

Brief Description of Policy (please attach copy if available). Please state if it is a new, existing or amended policy.

The amended policy outlines steps being taken by the Council to comply with the General Data Protection Regulation and Data Protection Act 2018.

Intended aims/outcomes. What is the policy trying to achieve?

To ensure Armagh City, Banbridge & Craigavon Borough Council's compliance with General Data Protection Regulation and the Data Protection Act 2018.

The Act is designed to safeguard the personal data held by Council regarding individuals and to protect them from the processing of incorrect data or the inappropriate processing of correct data held by Council.

Policy Framework

Has the policy been developed in response to statutory requirements, legal advice or on the basis of any other professional advice? Does this affect the discretion available to Council to amend the policy?

Policy is to ensure compliance with the General Data Protection Regulation and Data Protection Act 2018 and Information Commissioner's Office guidance thereon which affects the discretion available to Council to amend the policy.

Are there any Section 75 categories which might be expected to benefit from the policy? If so, please outline.

All categories will benefit from the policy.

Who initiated or wrote the policy (if Council decision, please state)? Who is responsible for implementing the policy?

Who initiated or wrote policy?	**Who is responsible for implementation?**
Senior Records Manager, (Armagh City, Banbridge and Craigavon Borough Council).	Officer(s) within Armagh City, Banbridge & Craigavon Borough Council with responsibility for data protection matters.

Are there any factors which might contribute to or detract from the implementation of the policy (e.g. financial, legislative, other)?

No.

Main stakeholders in relation to the policy

Please list main stakeholders affected by the policy (e.g. staff, service users, other statutory bodies, community or voluntary sector, private sector)

Staff/councillors Any other persons whose personal data is held by Council (e.g. service users).

Are there any other policies with a bearing on this policy? If so, please identify them and how they impact on this policy.

Access to Information policy; Records Management policy; Retention & Disposal Schedule.

Available Evidence

Council should ensure that its screening decisions are informed by relevant data. What evidence/information (both qualitative and quantitative) have you gathered to inform this policy? Specify details for each of the Section 75 categories.

Section 75 category	Evidence
Religious belief	None.
Political opinion	None.
Racial group	None.
Age	None.
Marital status	None.
Sexual orientation	None.
Men and women generally	None.
Disability	None.
Dependants	None.

Needs, experiences and priorities

Taking into account the information gathered above, what are the different needs, experiences and priorities of each of the following categories in relation to this particular policy/decision?

Section 75 category	Needs, experiences and priorities
Religious belief	Not applicable
Political opinion	Not applicable
Racial group	Not applicable
Age	Not applicable
Marital status	Not applicable
Sexual orientation	Not applicable
Men and women generally	Not applicable
Disability	Not applicable
Dependants	Not applicable

Screening Questions

1. What is the likely impact on equality of opportunity for those affected by this policy for each of the Section 75 categories?		
Category	Policy Impact	Level of impact (Major/minor/none)
Religious belief	None	
Political opinion	None	
Racial group	None	
Age	None	
Marital status	None	
Sexual orientation	None	
Men and women generally	None	
Disability	None	
Dependents	None	

2. Are there opportunities to better promote equality of opportunity for people within the Section 75 categories?		
Category	If yes, provide details	If no, provide reasons
Religious belief	N/A	
Political opinion	N/A	
Racial group	N/A	
Age	N/A	
Marital status	N/A	
Sexual orientation	N/A	
Men and women generally	N/A	
Disability	N/A	
Dependents	N/A	

3. To what extent is the policy likely to impact on good relations between people of different religious belief, political opinion, or racial group?		
Category	Details of Policy Impact	Level of impact (major/minor/none)
Religious belief	N/A	
Political opinion	N/A	
Racial group	N/A	

4. Are there opportunities to better promote good relations between people of different religious belief, political opinion or racial group?		
Category	If yes, provide details	If no, provide reasons
Religious belief	No	
Political opinion	No	
Racial group	No	

Multiple Identity

Generally speaking, people fall into more than one Section 75 category (for example: disabled minority ethnic people; disabled women; young Protestant men; young lesbian, gay and bisexual people). Provide details of data on the impact of the policy on people with multiple identities. Specify relevant Section 75 categories concerned.

Not applicable.

Disability Discrimination (NI) Order 2006

Is there an opportunity for the policy to promote positive attitudes towards disabled people?

No impact on any category.

Is there an opportunity for the policy to encourage participation by disabled people in public life?

Not applicable.

Screening Decision

A: NO IMPACT IDENTIFIED ON ANY CATEGORY – EQIA UNNECESSARY

Please identify reasons for this below

No impact on any category. This is a technical policy to ensure compliance with statutory requirements and good practice. EQIA unnecessary.

B: MINOR IMPACT IDENTIFIED – EQIA NOT CONSIDERED NECESSARY AS IMPACT CAN BE ELIMINATED OR MITIGATED

Where the impact is likely to be minor, you should consider if the policy can be mitigated or an alternative policy introduced. If so, an EQIA may not be considered necessary. You must indicate the reasons for this decision below, together with details of measures to mitigate the adverse impact or the alternative policy proposed.

N/A

C: MAJOR IMPACT IDENTIFIED – EQIA REQUIRED

If the decision is to conduct an equality impact assessment, please provide details of the reasons.

N/A

Timetabling and Prioritising

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

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

Priority criterion	**Rating (1-3)**
Effect on equality of opportunity and good relations	
Social need	
Effect on people's daily lives	

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 Council in timetabling its EQIAs.

Is the policy affected by timetables established by other relevant public authorities? If yes, please give details.

N/A

Monitoring

Effective monitoring will help the authority identify any future adverse impact arising from the policy. It is recommended that where a policy has been amended or an alternative policy introduced to mitigate adverse impact, monitoring be undertaken on a broader basis to identify any impact (positive or adverse).

Further information on monitoring is available in the Equality Commission's guidance on monitoring (www.equalityni.org).

Identify how the impact of the policy is to be monitored

There are no plans to monitor subject access requests by Section 75 category.

Approval and Authorisation

A copy of the screening form for each policy screened should be signed off by the senior manager responsible for that policy. The screening recommendation should be reported to the relevant Committee/Council when the policy is submitted for approval.

Screened by	**Position/Job title**	**Date**
Joan Farley	Senior Records Manager	10 January 2019
Approved by	**Position/Job Title**	**Date**

Please forward a copy of the completed policy and form to: mary.hanna@armaghbanbridgecraigavon.gov.uk who will ensure these are made available on the Council's website.

The above officer is also responsible for issuing reports on a quarterly basis on those policies "screened out for EQIA". This allows stakeholders who disagree with this recommendation to submit their views. In the event of any stakeholder disagreeing with the decision to screen out any policy, the screening exercise will be reviewed.

Appendix F - Rural Needs Impact Assessment

SECTION 1 - Defining the activity subject to Section 1(1) of the Rural Needs Act (NI) 2016

1A. Name of Public Authority

Armagh City, Banbridge and Craigavon Borough Council

1B. Please provide a short title which describes the activity being undertaken by the Public Authority that is subject to Section 1(1) of the Rural Needs Act (NI) 2016.

Data Protection Policy

1C. Please indicate which category the activity specified in Section 1B above relates to

Developing a	Strategy		Policy		Plan	
Adopting a	Strategy		Policy		Plan	
Implementing a	Strategy		Policy		Plan	
Revising a	Strategy		Policy	x	Plan	
Designing a Public Service						
Delivering a Public Service						

1D. Please provide the official title (if any) of the Strategy, Policy, Plan or Public Service document or initiative relating to the category indicated in Section 1C above

Data Protection Policy

1E. Please provide the aims and/or objectives of the Strategy, Policy, Plan or Public Service

This document sets out the appropriate actions and procedures which must be followed to comply with the General Data Protection Regulation and the Data Protection Policy 2018 by Armagh City, Banbridge and Craigavon Borough Council.

1F. Which definition of 'rural' is the Public Authority using in respect of the Policy, Strategy, Plan or Public Service?

Population Settlements of less than 5,000 (Default definition)	
Other Definition (Provide details and the rationale below)	
A definition of 'rural' is not applicable	x

Details of alternative definition of 'rural' used

Rationale for using alternative definition of 'rural' used

SECTION 2 – Understanding the impact of the Policy, Strategy, Plan or Public Service

2A. Is the Policy, Strategy Plan or Public Service intended to impact on people in rural areas?

YES [ ] **NO** [x] **If the response is NO GO TO Section 2E**

2B. Please explain how the Policy, Strategy, Plan or Public Service is intended to impact on people in rural areas

2C. If the Policy, Strategy, Plan or Public Service is intended to impact on people in rural areas differently from people in urban areas, please explain how it will impact people in rural areas differently

2D. Please indicate which of the following rural policy areas the Policy, Strategy, Plan or Public Service is intended to impact on

Rural Businesses	☐
Rural Tourism	☐
Rural Housing	☐
Jobs or Employment in Rural Areas	☐
Education or Training in Rural Areas	☐
Broadband or Mobile Communications in Rural Areas	☐
Transport Services or Infrastructure in Rural Areas	☐
Health or Social Care Services in Rural Areas	☐
Poverty in Rural Areas	☐
Deprivation in Rural Areas	☐
Rural Crime or Community Safety	☐
Rural Development	☐
Other (Please state)	☐

If the response to Section 2A was YES GO TO Section 3A

2E. Please explain why the Policy, Strategy, Plan or Public Service is NOT intended to impact on people in rural areas

This is a technical policy written to ensure compliance with statutory requirements and good practice. It is not intended to impact on people in rural areas.

SECTION 3 – Identifying the Social and Economic Needs of Persons in Rural Areas

3A. Has the Public Authority taken steps to identify the social and economic needs of people in rural areas that are relevant to the Policy, Strategy, Plan or Public Service?

YES [ ] NO [x] **If the response is NO GO TO Section 3E**

3B. Please indicate which of the following methods or information sources were used by the Public Authority to identify the social and economic needs of people in rural areas

Consultation with rural stakeholders	☐	Published statistics	☐
Consultation with other organisations	☐	Research papers	☐
Surveys or questionnaires	☐	Other publications	☐

Other methods of information sources (include details in section 4 below).

3C. Please provide details of the methods and information sources used to identify the social and economic needs of people in rural areas including relevant dates, names of organisations, titles of publications, website references, details of surveys or consultations undertaken etc.

3D. Please provide details of the social and economic needs of people in rural areas which have been identified by the Public Authority?

If the response to Section 3A was YES GO TO Section 4A

3E. Please explain why no steps were taken by the Public Authority to identify the social and economic needs of people in rural areas??

This is a technical policy written to ensure compliance with statutory requirements and good practice. It is not intended to impact on people in rural areas.

SECTION 4 – Considering the Social and Economic Needs of Persons in Rural Areas

4A. Please provide details of the issues considered in relation to the social and economic needs of people in rural areas identified by the Public Authority.

N/A

SECTION 5 – Influencing the Policy, Strategy, Plan or Public Service

5A. Has the development, adoption, implementation or revision of the Policy, Strategy or Plan, or the design or delivery of the Public Service, been influenced by the rural needs identified?

If the response to 5A was YES COMPLETE 5B then GO TO Section 6A

YES [ ] **NO** [x] **If the response is NO GO TO Section 5C**

5B. Please explain how the development, adoption, implementation or revision of the Policy, Strategy or Plan, or the design or delivery of the Public Service, has been influenced by the rural needs identified

5C. Please explain why the development, adoption, implementation or revision of the Policy, Strategy or Plan, or the design or the delivery of the Public Service, has NOT been influenced by the rural needs identified

This is a technical policy written to ensure compliance with statutory requirements and good practice. It is not intended to impact on people in rural areas.

SECTION 6 – Documenting and Recording

6A. Please tick below to confirm that the Rural Needs Impact Assessment will be recorded on the Public Authority's Annual Monitoring Return and the RNIA Template retained by the Public Authority

I confirm that details of the Rural Needs Impact Assessment will be recorded and the RNIA Template retained	**x**

Rural Needs Impact Assessment undertaken by:	Joan Farley
Position	Senior Records Manager
Department	Governance and Democratic Services
Signature:	
Date:	10.01.19
Rural Needs Impact Assessment approved by:	Eamonn Kelly
Position:	Head of Governance and Democratic Services
Department/Directorate	Performance
Signature:	
Date:	