Douglas

Douglas City Council

GENERAL DATA PROTECTION & CONFIDENTIALITY POLICY

(GDPR)

Policy Review - History:
Please be aware that a hard copy of this document may not be the latest available version, which is available on the Council's Intranet, and which supersedes all previous versions.

Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for always complying with policy requirements.

Effective from:	**Replaces:**	**Originator:**	**Page X of Y**
August 2018	Draft Version 2011	ACO (D&I) / COMT	1 of 16
Chief Officers' Management Team Approval:		July 2024	
Union the Union & Unison Union Agreement:		N/A	
Executive Committee Approval:		N/A	
Council Ratification:		N/A	

History or Most Recent Policy Changes – MUST BE COMPLETED		
Version:	Date:	Change:
1.0	July 2018	Significant Re-write of Data Protection Policy (2011)
2.0	June 2024	Borough to City, DBC to DCC; remove annual notifications to ICO; add Annual Registration to Information Commissioner and remove section on fees. Added Breach Notification flowchart.

CONTENTS:

1. Introduction 03

2. Requirements of Legislation & Definitions 03

3. GDPR Principles 05

4. Douglas City Council Responsibilities 06
   - 4.1 Staff Training and Awareness 06
   - 4.2 Annual Registration to Information Commissioner 07
   - 4.3 Managing the Right of the Data Subject 07
   - 4.4 Breach Reporting 09
   - 4.5 Information Security 10
   - 4.6 Document Retention Schedule and Disposal Policy 10
   - 4.7 Data Protection Impact Assessments (DPIA's) 10
   - 4.8 Data Protection 'Privacy by Design' 11

5. Data Accuracy 11
   - 5.1 Audit and Control 12

6. Privacy Statements 12

7. Appendix A 13

8. Appendix B 14

9. Appendix C 16

1. Introduction

This policy sets out the way in which Douglas City Council (DCC) will collect, store, manage and share private personal information about the people for whom it provides a service and with whom it works. Because of the broad range of activities and functions undertaken by the Council it is necessary to use personal information for a wide variety of reasons.

It is a general principle of the Council's General Data Protection Policy that private information will be treated with respect and a level of confidentiality appropriate to the type of information and the reason it is used. This general expectation of confidentiality should apply in all cases except where it is shared to meet a legitimate function of the Council such as an overriding public interest, a legal obligation, or in the interests of the person themselves.

This policy is made up of several documents. These documents will be updated on a regular basis following any organisational change where the use of personal data has changed e.g., introduction of a new service.

Documents that make up this policy include the following: -

1. Douglas City Council GDPR Policy (this document)
2. Douglas City Council Privacy Policy (2024)
3. Douglas City Council Document Retention Schedule and Disposal Policy (2023)
4. Douglas City Council Human Resources GDPR Policy (2024)
5. Douglas City Council Human Resources Records Retention Policy (2024)
6. Douglas City Council Digital Services Staff Usage and Security Policy (2024)
7. Douglas City Council Isle of Man Local Government Superannuation Scheme Privacy Policy (2024)

This policy will also reference the legislation. A link to the legislation can be found on the Information Commissioners website: -

www.inforights.im

The legislation is made up of articles; each of these articles reference a particular focus of the legislation. The articles are supported by several recitals that explain the reasoning behind a decision. These are very useful for reference and understanding.

The www.Inforights.im website also contains several useful guides around specific data topics.

The UK website https://ico.org.uk/ is also an excellent website for reference material in relation to the legislation.

The following website has an excellent interaction version of the EU Legislation.

https://gdpr-info.eu

2. Requirements of Legislation & Definitions

The chief requirements outlined in this policy are based upon the 2018 GDPR Regulation (GDPR), which is the central piece of legislation covering security and confidentiality of personal information.

The GDPR imposes obligations on the use of all personal information held by organisations such as the Council. The act contains several important definitions which are set out below. It is important to understand these definitions as they will be used in this policy.

Data Protection Legislation: The Isle of Man GDPR 2018.

Personal data: The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g., key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal data: The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Data Subject:
An identifiable natural living person who can be identified, directly or indirectly, by reference to an identifier such as name, identification number, location data, online ID, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

Confidential Information:
Information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory) relating to the business, products, affairs and finances of the Company for the time being confidential to the Company and trade secrets including, without limitation, technical data and know-how relating to the business of the Company or any of its business contacts, including in particular (by way of illustration only and without limitation).

Data Controller:
The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; Douglas City Council is a Data Controller.

The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. So, if our company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within our organisation do so to fulfil our tasks as data controller.

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

Joint Data Controller:
DCC is a **joint controller** when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed. An example for the Council would be Douglas Golf Club where the Club and Douglas Council are both required to process the data for a golf club member.

Data Protection Officer ('DPO'):
The DPO will assist Managers and staff to monitor internal compliance, inform and advise on Council data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Data subjects shall have the right to contact the DPO on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

Information Commissioner (IC):
The Information Commissioner is the independent authority responsible for upholding the public's information rights and promoting and enforcing compliance with the Island's information rights legislation, which includes the Freedom of Information Act, GDPR and Unsolicited Communications Regulations.

3. Data Protection Principles

Douglas City Council processes personal data in accordance with the following data protection principles:

- DCC processes personal data lawfully, fairly and in a transparent manner;
- DCC collects personal data only for specified, explicit and legitimate purposes;
- DCC processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- DCC keeps accurate personal data and takes all reasonable steps to ensure that inaccurate data is rectified or deleted without delay;
- DCC keeps personal data only for the period necessary for processing; and
- DCC adopts appropriate measures to ensure that personal date is secure, protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

How the Council complies with the data protection principles is detailed in the Douglas City Council Privacy Policy (2024), Human Resources (HR) GDPR Policy (2024), Digital Services Staff Usage and Security Policy (2024) and Local Authority Superannuation Scheme Privacy Policy (2024).

These policies are available directly from the Councils website www.Douglas.gov.im/Dataprotection

Managers are responsible for ensuring that their Department or Section are adhering to the Policies.

The DPO should be consulted for approval in all cases where a privacy notice is to be used.

4. Douglas City Council Responsibilities

The Chief Executive has overall responsibility for GDPR within the Council.

The implementation of this policy is overseen by the DPO. This role is assigned to the Assistant Chief Officer (Democratic Services), who has the responsibility for ensuring it is implemented and operated correctly across the organisation.

The DPO is also responsible for investigating incidents involving breaches or potential breaches of information security and providing advice.

Whilst the Chief Executive and the DPO have the responsibilities outlined above, **all Managers** are responsible for ensuring that this policy is communicated and implemented across their area of responsibility.

The Managers are responsible for the quality, security and management of personal data in use in their area including carrying out risk assessments and providing reports for the DPO on measures taken to mitigate or deal with information risks. Advice or assistance regarding this policy or GDPR in general is available to them from the DPO. Excellent guidance is also provided by the Office of the Information Commissioner on their website at https://www.inforights.im/

Training will be provided where required, this can be processed in line with the Council's training programme/staff development review. Further information can be found in the HR GDPR Policy (2024).

All subject access request is to be reported to the DPO, they should be complied with by the Department or Section processing the relevant data. The DPO will provide advice and guidance as necessary. The process is outlined in Appendix A.

Where personal data is regularly shared by the Council for specific purposes with other organisations, Information Sharing Agreements will be prepared by the appropriate officer and signed on behalf of the Council by the DPO. Advice can be provided by the DPO.

All data protection and information related breach incidents should be reported immediately to the DPO and managed according to the Council's Data Protection Breach process. The breach reporting process is detailed in Appendix B.

All correspondence with the Information Commissioner's Office on GDPR matters will be dealt with by the DPO or Deputy DPO in their absence.

This Policy will be reviewed annually by the DPO to coincide with the annual requirement to register with the Office of the Information Commissioner, and when appropriate to consider lessons learned from any actual or potential data protection or confidentiality breaches, changes to legislation or guidance from the Information Commissioner.

4.1. Staff Training and Awareness

Training will be provided to all employees about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Employees whose roles require regular access to personal data, or who are responsible for implementing this policy, or are responding to subject access requests under this policy, will receive additional training.

The DPO will send out regular communications to all staff in relation to data protection awareness.

4.2. Annual Registration to IC

The Council must register as a Controller (on the 1st May each year) to the IC. As a Controller the Council must implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary ... the measures ...shall include the implementation of appropriate data protection policies by the controller. Compliance must be readily demonstrable to individuals and supervisory authorities and failure to do so may lead to sanctions and/or a fine of up to £1,000,000.

The Assistant Chief Officer (Democratic Services) is responsible for submitting the annual registration. All managers must carry out an annual review of their data use and notify the Assistant Chief Officer (Democratic Services) if the type of personal data their Department holds or the way it is managed changes significantly.

4.3. Managing the Rights of the Data Subject

Under GDPR law the data subject has several rights in relation to the personal information that is held about them. These include: -

Right of Access and Subject Access Requests (SAR)
A data subject has the right to ask for copies of personal information held relating to them. This right always applies. There are some exemptions, which will be evaluated on submission of the request.

Right to Rectification
A data subject has the right to ask for information to be rectified if they think it is inaccurate. They also have the right to ask for information they think is incomplete to be completed.

Right to Erasure
A data subject has the right to ask for their personal information to be erased in certain circumstances. Only data that is no longer required for the purposes it was collected should be deleted. This will always be reviewed by the DPO for validity.

Right to Restriction of Processing
A data subject has the right to ask for the processing of information to be restricted in certain circumstances.

Right to Data Portability
This applies to information supplied to DCC by the data subject. A data subject has the right to ask for the information they gave us to be transferred to another organisation or supply it direct to them.

The above rights will come to DCC as formal requests, definitions of these requests can be found in the Council's Privacy Policy.

This section defines how DCC will process the requests from the data subject.

A data subject has the right to make these requests only for data relating to themselves. No request should be processed if there is a possibility that by performing the task another individual can be identified. Refer to the DPO for guidance on specific cases.

There are several clear rules and guidelines that relate to these requests:

- There is no fee
- Requests must be replied to within one month (if a request is complex the Council can extend the time period for responding by a further two months) *
- If the request is made electronically the response must also be issued electronically
- There is no set format for a request, however the Council will assist by provided pre-formatted forms/e-forms
- The response may also provide the following information (depending on the type of request)**:**
    - the purposes of processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient disclosed the personal data to;
    - retention period for storing the personal data or, where this is not possible, criteria for determining how long it is stored;
    - the existence of their right to request rectification, erasure or restriction or to object to such processing;
    - the right to lodge a complaint with the ICO or another supervisory authority;
    - information about the source of the data, where it was not obtained directly from the individual;
    - the existence of automated decision-making (including profiling); and
    - the safeguards provided if personal data is transferred to a third country or international organisation.

* DCC can extend the time to respond by a further two months if the request is complex or several requests have been received from the individual. DCC must let the individual know as soon as possible or within one month of receiving their request and explain why the extension is necessary.

Making the request
Although there is no requirement to fill out an official form to submit a SAR, the Council have provided an electronic form to make the submission of a request easier. See www.Douglas.gov.im/Dataprotection

Regardless of the format used, the following information should be provided to identify the individual and assist with the search:

- Full name, title and date of birth;
- Current address and previous addresses (reasonable for identification purposes only);
- Specific details of the request, e.g., for a SAR request not all requesters will require all data; and

- Any other data that may assist in the identification of the individual or the data required e.g., Account numbers, previous names etc.

Before a request can be processed the individual ***may*** need to prove who they are. The standard approach to verification of identity will be in the form of 2 forms of ID:

- One must be a Utility bill issued in the last 3 months; and
- One must be a form of photo ID, either driving licence or passport.

If the person does not have any of the above, then the request should be reviewed by the DPO to identify other possible forms of acceptable identification.

In certain circumstances DCC may be satisfied that the individual is known to them, and this level of identification will not be required e.g., housing tenant where ID data is already held.

Exemptions to the ID process exist for Council employees, please see the HR GDPR Policy (2024) for specific details.

Although the Council will publish contact details for submitting a request (see Privacy Policy) a request could come into any team or individual directly in any format.

To assist with the understanding around the processing of the requests a flow chart is attached (Appendix A – Process Charts).

Third Party Requests
The GDPR legislation does not prevent an individual from making a request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, DCC need to be satisfied that the third party making the request is entitled to act on behalf of the individual, and it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a power of attorney.

If processing personal information for criminal law enforcement purposes, the rights of the data subject are slightly different.

A flow chart showing the management process for requests can be found at Appendix A.

4.4. Breach Reporting

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. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data (system failure).

Typical real-world examples may include: -

- Sending unencrypted data within an email to the wrong person;
- Losing a USB stick containing personal data;
- Leaving print outs containing personal data in a public area;
- Sending a letter to the wrong person; and
- Computer systems being hacked.

The legislation requires any data breach to be reported to the Information Commission within **72 hours** of the breach being reported/identified.

When a personal data breach has occurred, it is necessary to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then DCC must notify the IC; if it is **unlikely then it does not have to be reported.**

However, if it is decided that the breach does not need to be reported this decision needs to be justifiable therefore, it needs to be documented.

In the event of any suspected breach, it should be reported immediately to the DPO or Deputy DPO in their absence.

To assist with the documenting and identification of the data breach a Data Breach Reporting Form is attached (Appendix B).

4.5. Information Security

The Council's Information security process is defined in the Digital Services Staff Usage and Security Policy (2024).

4.6. Document Retention

The Council's records management responsibilities are defined in the Council's Document Retention Schedule and Disposal Policy (2023).

4.7. Data Protection Impact Assessments (DPIA's)

It is important that when engaging with a new project, changes to the way that we manage personal data are taken into consideration.

A DPIA is a way to systematically and comprehensively analyse processing and help identify and minimise data protection risks. You can think of it as an audit of the process that highlights any risks to personal data.

DPIAs should consider compliance risks, and the 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, 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 (Risk Assessment).

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. An effective DPIA can bring broader compliance, financial and reputational benefits, helping to demonstrate accountability and building trust and engagement with individuals.

In the very first instance of change all Officers should be thinking about the possible impact on personal data. If it is considered that personal data will be impacted in any way, then it is advisable to contact the DPO.

A full DPIA review is only required should there be significant high risk to personal data. An example would be the Council's introduction of a new Car Park system. This system processes personal data and identifies when a person is in a location; this data is then stored for a period. This is a good example of where a DPIA should be used to assess the impact on the individuals.

4.8. Data Protection 'Privacy by Design'

Data protection 'privacy by design' is another requirement of the legislation.

It is very tightly linked to the DPIA assessments in as much as it requires us to consider the privacy requirements of data in all things that we do, this includes existing systems/processes and new processes/systems.

This is very much a requirement of the organisation as a whole. The legislation is really trying to make sure that organisations change their cultures and start to include the 'thinking about privacy' actions in everything they do.

Where a change is identified as a higher risk, consideration should be given to the DPIA process.

Not considering a change in this way may risk not carrying out the necessary review; ultimately this could result in DCC operating unlawfully. It is important to embed this thought process into everything we do.

5. Data Accuracy

Managers are responsible for ensuring that data collected from or about data subjects is complete and fit for purpose.

Staff using Information systems including databases and manual filing systems should receive specific training from the section Manager (or an appropriate Officer nominated by the section Manager) on their use to ensure that information which is required to make decisions about people is accurately and adequately recorded. Standard glossaries and explanations of abbreviations should be available, especially when information is shared between teams and departments.

Wherever a hybrid system of manual and computer records are used in a single environment, guidance must be produced to ensure that staff understand how and when to record information on either or both systems. The purpose of both systems must be clear and understood.

Managers must ensure that personal data held in any form is accurate and up to date. Data subjects should regularly be consulted about whether the information held about them is still current. This will be dependent on the process and the reasons as to why the data is being held. Please refer to the DPO for further guidance.

Application forms and other data gathering tools and processes should be reviewed regularly to ensure that they still gather sufficient information, and do not contain questions which are no longer relevant to the service.

Managers should notify the Assistant Chief Officer (Democratic Services) if personal data is to be used for a new purpose which is materially different to that for which it was obtained, to consider whether the use is valid.

5.1. Audit and control

The Council will conduct periodic compliance audits of major services and processes to ensure that this policy and the GDPR are complied with.

Any questions relating to this policy should be directed to the Councils' DPO.

6. Privacy Statements

It is important that at any point where data is collected the DCC Privacy Policy is referenced. There are two privacy statements that should be used. The standard statement can be used across all services with the exclusion of Housing.

The Housing statement should be used when dealing with tenant/housing related processes.

There is an additional statement to be added when collecting data from third person e.g., when another individual's details are provided by somebody else e.g., collection of lodger details on a Housing form.

These statements are attached (Appendix C).

7. APPENDIX A

Douglas

Douglas City Council

Douglas City Council – Data Subject Request Process

A data subject can make a number of requests to the Council, these include a request to receive all of their data, a request for deletion or a request to stop processing. It is important that when dealing with the request a standard process is followed. This process defines high level the steps that need to be taken when processing a request.

All requests should be dealt with within <u>one calendar month</u>.

Request received?

All received requests should be passed to the Data Protection Officer (DPO) immediately. Please phone the DPO officer **immediately** so they are aware a request has arrived. The email address is Dataprotection@Douglas.gov.im

Request reviewed by Data Protection Officer

The DPO will review the request for validity and will also confirm if the identity of the requester or any other information needs to be confirmed.

Capture the record of request

The Data Protection Officer will log the details of the request. The request should be responded to within one month.

Instruction request issued

The DPO will now instruct the relevant Officer to carry out the request. The details required to carry out the task need to be delivered to the Officer for the purpose of the action only. Depending on the request type the DPO will define the period of time by which the request or part request needs to be completed.

Request can now be delivered to the department(s) who hold the data

Request should be managed by one responsible Officer who can co-ordinate the actions.

We need to make sure we have searched thoroughly

It is the responsibility of the Officer to make sure the request is completed in its entirety. In most situations the request will relate to the information of the Data Subject and therefore completeness in the search for their data is very important.

Prepare for the request action

It is important to determine how and if the request can be processed. In certain circumstances there may be the opportunity to do part but not all of the request, pull together a plan of actions for performing the request and submit to the Councils DPO.

DPO review the action plan for the request

The DPO will review the request and look to resolve any issues. The DPO will also review if there are any exemptions that will need to be applied to the request.

Action the request

Following confirmation from the DPO the Officer should action the request. This may range from a SAR search to processing a suspension and therefore different actions will require different time periods to implement. Once complete the DPO should be informed.

DPO to inform data subject

The DPO will review the output of the actions and inform the data subject of the results. This may involve the delivery of information. The DPO must also explain to the data subject their rights of appeal.

Data subject receives response

The Data Subject may decide to appeal any response.

<u>KEY</u>

Data Subject **DPO Officer** **Council Officer**

If you have any queries please contact the DPO Officer – Linda Radcliffe on 696310 or email Dataprotection@Douglas.gov.im

8. APPENDIX B

Information Breach Report Form

This form is for managers and/or senior managers to complete following the initial report of an information incident. It should not take more than 15 minutes to complete.

If you are unsure about the procedures for managing an information incident, you should refer to the Council's GDPR policy that can be found on the Intranet.

Please provide as much information as possible. If you do not know the answer or you are waiting on the completion of further enquiries, please state this and indicate when this information may be available. In addition to completing the form below, please provide any other supporting information that maybe relevant. If you are unsure about anything then contact the DPO in the first instance, call 696 (310) or email Dataprotection@Douglas.gov.im

Should there be an information incident, swift containment and recovery of the situation is vital. Every effort should be made to minimise the potential impact on affected individuals and the Council, and details of the steps taken to achieve this should be included in this form.

Please do not delay in sending this form to the DPO, email Dataprotection@Douglas.gov.im

Contact Details

Please provide your full name, please note that all information will be kept confidential in relation to this breach report and any further actions.

Full Name	
Phone	
E-mail address	

a) Details of the information incident

1. Please describe the incident/breach in as much detail as possible.
2. Please give details of when the incident/breach happened. Please note data and time where possible, if there are multiple incidents, please detail all dates.
3. If there has been a delay in reporting the incident to the DPO please explain why.
4. What were the control factors in place to prevent this from happening, it there were none then please state 'none'.

b) Personal data placed at risk

1. What, if any, personal data has been placed at risk? Please specify if any financial, commercial or personal sensitive data has been affected and provide details of the extent.
2. How many individuals (Data subjects) have been affected?
3. Have the affected individuals been made aware that an incident has occurred? Please state whether their awareness was 'formal' e.g., informed them directly or 'they have discovered through other means' that their data was compromised.

4. What are the potential risks, consequences and adverse effects on those individuals?

5. Have any of the affected individuals complained about the incident and if so, what action has been taken?

c) Containment and Recovery

1. Has any action been taken to minimise/mitigate the effect on the affected individual(s)? If so, please provide details.
2. Has the information placed at risk now been recovered? If so, please provide details of how and when this occurred.
3. Have any steps been taken to prevent a recurrence of this incident? If so, please provide details.
4. Who have you informed about the incident, internally and externally? For example, in the event of theft, have the Police been informed and do you have a crime number?

d) Training and Guidance

1. Please confirm that all employees involved with the incident have successfully completed the Council's Data Protection training.
2. Has any additional Information relating to Governance training been provided? If so, please provide details.
3. Has any specific detailed operational guidance been developed and provided to staff on handling information, including the use of Council IT equipment? If so, please provide details.

e) Investigation (may not yet be done)

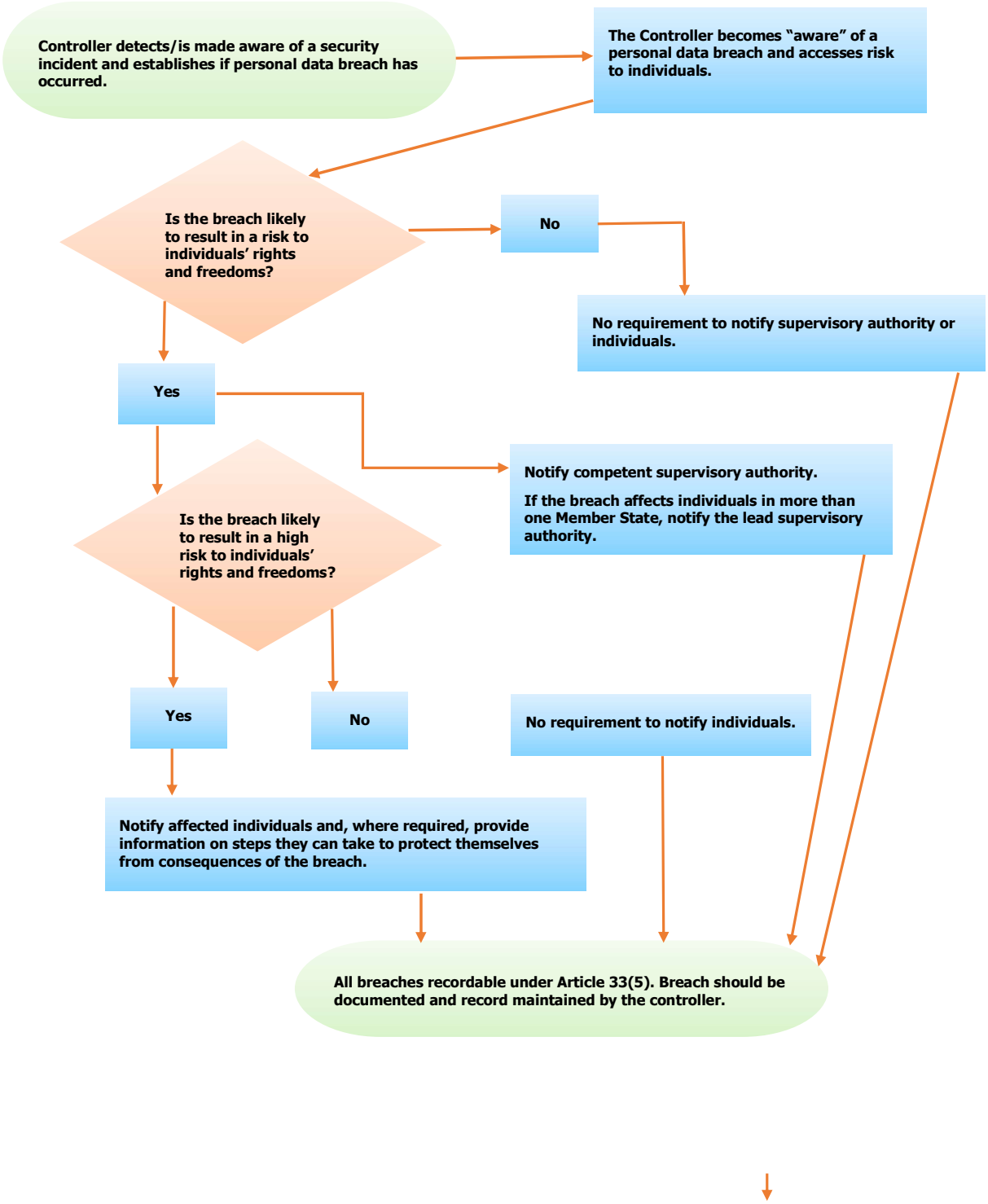
1. What, if any actions have been taken to preserve evidence and/or create an audit trail relating to the information incident?
2. What, if any, remedial actions have been taken since the information incident occurred to prevent any recurrence?
3. Where remedial actions have been identified what timescales have been agreed for implementation? Please provide details.
4. Where remedial actions have been identified what timescales have been agreed for implementation? Please provide details.

What happens next?

When the form is received, the DPO will contact you to provide:

- An incident reference number; and
- Information about our next steps and further information that may be required for the investigation

Data Breach Notification Flowchart



9. APPENDIX C

Standard Privacy Statement

"Douglas City Council collects personal data in accordance with the relevant GDPR legislation. Should you wish to learn more about this please read our Privacy Policy which clearly sets out what personal information is collected, why, and for how long. The Privacy Notice can be located at *www.douglas.gov.im/dataprotection*, and can also be requested in person at the reception at Douglas City Hall. Further, should you have any specific questions please do not hesitate to contact our DPO at *dataprotection@douglas.gov.im* or phone 01624 696310."

Additional Statement When Collecting Additional Person's Data

When you provide us with information about another person lawful basis for processing this personal information is that it is necessary for compliance with a contract and/or legal obligation, that it is necessary for the performance of a task carried out in the public interest and/or necessary in the exercise of official authority vested in Douglas City Council."

Housing Privacy Statement

"COMMITMENT - Douglas City Council is fully committed to complying with the requirements of current data protection legislation as applied in the Isle of Man. Ensuring the security and protection of all personal information that we collect and process in accordance with the relevant data protection legislation and our own Data Protection Policy. This includes collecting and processing personal data for the purpose of carrying out checks, for the purposes of administration, assessment, analysis, and also for assessing tenant (and prospective tenant) suitability for housing and/or general housing management. Personal data collected may include details of any criminal convictions, on-going investigations, health data, family background data and to make any necessary enquiries to check that information contained in the Tenancy Agreement/Housing Application Form is correct and for the purposes described above.

Douglas City Council may, in accordance with the relevant data protection legislation and its Data Protection Policy, share this personal information with law enforcement, government agencies, government departments, local authorities, contracted third-party service providers, financial companies and/or financial organisations.

For further information please read our main Privacy Notice which explains how we collect, store and handle your personal data as well as your rights. If you would like to find out more, please visit our website at http://www.douglas.gov.im/dataprotection or request in person at Douglas City Hall.

Should you have any specific questions about this statement please do not hesitate to contact our ***Data Protection Officer*** *at Dataprotection@Douglas.gov.im or telephone 01624 696300.*

If you would like to know more about current data protection legislation, you can contact the Information Commissioner at https://www.inforights.im/ or by ringing 01624 693260."

Additional Housing Statement When Collecting Additional Person's Data

When you provide us with information about another person in your Housing application/change Form our lawful basis for processing this personal information is that it is necessary for compliance with a contract and/or legal obligation, that it is necessary for the performance of a task carried out in the public interest and/or necessary in the exercise of official authority vested in Douglas City Council."