



Commissioner for **Older People**
for Northern Ireland

Data Protection and Security Policy

Date Reviewed	October 2020
Approved by the Chief Executive	Evelyn Hoy
Date:	26 October 2020
Approved by the Accounting Officer	Eddie Lynch
Date:	14 December 2020
Periodic Review Date	October 2022
Version	7

Contents

1 Introduction 3

2 Statement of Policy 3

3 Data Protection Principles..... 3

4 Disclosure of Personal Information 4

5 Handling of Personal Information..... 5

6 Compliance**Error! Bookmark not defined.**

7 Staff Responsibilities..... 6

8 Third Party Users of Personal COPNI Information..... 6

9 Data Breaches 7

10 Data Sharing..... 9

11 Individuals' Rights..... 9

12 Making a Subject Access Request 10

13 Policy Awareness 11

14 Policy Review 12

1 Introduction

The Commissioner for Older People for Northern Ireland (COPNI) is fully committed to complying with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) 2018. COPNI will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal or sensitive personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the Act. COPNI will also ensure the rights of the individual are at the core of our data protection policies and procedures.

2 Statement of Policy

COPNI may need to collect and use information about people with whom we work with in order to carry out our business and provide our services. These may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, COPNI may be required by law to collect and use such information. All personal information must be handled and dealt with properly, however it is collected, retained and used, and whether it is within manual files, in computer records or retained by any other means.

3 Data Protection Principles

COPNI fully support and comply with the six principles of the 1998 Act. In summary, this means personal information must be:

- a. processed fairly and lawfully;
- b. processed only for one or more specified and lawful purposes;
- c. adequate, relevant and not excessive for that purpose;
- d. kept accurate and up to date;
- e. kept for no longer than is necessary;
- f. kept and maintained securely; and
- g. .

Our purpose for holding personal information and a general description of the categories of people and organisations to which COPNI may disclose it are listed in the Information Commissioner's Office Data Protection Register.

4 Accountability and Compliance

COPNI will demonstrate compliance with the GDPR principles by ensuring that:

- data protection policies are implemented and adhered to;
- techniques such as data protection by design and data protection impact assessments are adopted;
- there is a designated Data Protection Officer (DPO) in the organisation;
- all staff complete data protection awareness as part of the induction process on appointment and will attend an awareness session regularly;
- everyone managing and handling personal information understands that they are directly and personally responsible for following good data protection and records management practice;
- only staff who need access to personal information as part of their duties are authorised to do so;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information knows who to speak to and where to seek advice;
- queries about handling personal information are promptly and courteously dealt with;
- a regular review (audit) is made of the way personal information is collected, held and processed;
- methods of handling personal information are monitored and reported to Management;
- performance on handling personal information is regularly monitored and reported to Senior Management.

5 Disclosure of Personal Information

Strict conditions apply to the transfer of personal information both internally (within COPNI) and externally (to any other person or body). COPNI will not disclose

personal information it holds to any third party unless COPNI believes it is lawful to do so. Confidentiality of personal information will be maintained, except where appropriate for lawful and permitted purposes, or where explicit consent to breach confidentiality has been sought and granted (for example in legal casework). In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- COPNI have the statutory power or are required by law to do so; or
- a member of staff has consented to the disclosure of their personal information; or
- the information is in a form that does not directly or indirectly identify individual employees or stakeholders.

6 Handling of Personal Information

All our staff will, through appropriate training and responsible management:

- fully observe conditions regarding the fair collection and use of personal and sensitive personal information;
- meet our legal obligations to specify the purposes for which personal information is collected and processed;
- collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of personal information used is as accurate as possible;
- apply strict checks and appropriate data retention and destruction schedules to determine the length of time personal information is held and how it is destroyed;
- ensure that the rights of people about whom information is held can be fully exercised under the Act;
- respond to Subject Access Requests promptly and within the one month deadline;
- take appropriate technical and organisational security measures to safeguard personal information. This includes ensuring group emails use

blind carbon copy for addresses and using the secure VPN or encrypted USB's to access sensitive personal information;

- ensure that personal information is not transferred to countries outside the UK without adequate safeguards;
- ensure all personal data is held in line with COPNI records management policy.

7 Staff Responsibilities

All staff have a responsibility to protect the personal information held by COPNI. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss, disclosure or destruction and in particular will ensure that:

- they are appropriately trained in the handling of personal information;
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords which have forced changes every 90 days;
- individual computer passwords are strong. Strong passwords are defined as being at least ten characters long; and containing two of the following – a capital letter, a number or a special character.

If and when, as part of their responsibilities, staff collect information about other people, they must comply with the guidance set out in this policy. No one should disclose personal information outside this guidance or use personal data held on others for their own purposes.

8 Third Party Users of Personal COPNI Information

Any third parties who are users of personal information supplied by COPNI will be required to confirm and demonstrate that they will abide by the requirements of the 1998 Act and the General Data Protection Regulation 2018. Audits will be carried out by COPNI on a regular basis to ensure compliance. Data processing/sharing agreements will be put in place when required.

9 Data Breaches

A data breach can happen for a number of reasons. Some examples are set out below but are not exhaustive:

- Loss or theft of information/papers containing personal information
- Loss or theft of equipment/mobile devices on which personal data is stored
- Emailing/faxing personal data to the wrong recipient
- Sending personal data by post to the wrong address/recipient
- Failure to encrypt laptops/equipment containing personal data
- Failure to apply appropriate access controls
- Failure to securely dispose of personal information
- Inaccurately recording personal data
- Inappropriate disclosure of personal data to a third party

In the event of a data breach, staff should inform the Data Protection Officer immediately. Once it has been confirmed that a breach has occurred the Data Protection Officer will carry out an investigation. This investigation will cover four key elements:

- Containment and recovery – this may involve the Data Protection Officer, IT Officer and Communications staff. This element will establish who needs to be made aware of the breach and what they need to do to assist in containment – i.e. changing passwords or finding a lost item of equipment or post. It will further establish if anything can be done to recover any losses and limit any damage the breach can cause. As well as the physical recovery of equipment or papers, this could involve the use of back up tapes to restore lost or damaged data.
- Assessment of risks – before deciding on the steps required, the DPO will assess the risks which may be associated with the breach especially an assessment of potentially adverse consequences for individuals, how serious these are and how likely they are to materialise. Consideration should be given to the following factors:
 - What type of data is involved?

- How sensitive is it?
 - Is the information protected, such as encryption?
 - What has happened to the information – stolen, lost, damaged?
 - How many people are affected?
 - Whose data has been breached – staff, customers, suppliers? This will help determine the level of risk posed by the breach and also the actions to mitigate the risks;
 - What harm can come to the individuals? Risks to physical safety or reputation or financial loss?
 - Are there wider consequences to consider such as loss of public confidence in a service we provide?
 - If bank details have been lost, consider contacting banks for advice on anything they can do to prevent fraudulent use
- Notification of breach (to individuals and other parties) – notification should have a clear purpose – to inform people (parties whose information security has been breached) of the breach and to allow them to take steps to protect themselves in as timely a manner as possible. Consideration should be given to who should be notified, what they should be told and how you are going to communicate the message. All such notifications must be approved by the CEO or Commissioner.
 - Evaluation and response – it is important to investigate the causes of a breach and also to evaluate the effectiveness of your response to it. If there are systemic problems, or inadequate policies or a lack of a clear allocation of responsibility, then it is important to ensure these are reviewed and updated.

Where appropriate, data breaches of personal information should be notified to the Information Commissioner's Office within 72 hours of becoming aware of the breach, where feasible. The Data Protection Officer will notify the ICO by email at casework@ico.org.uk. The notification should include;

- The type of information and the number of records;
- The circumstances of the loss/release/corruption;

- Actions taken to minimise/mitigate the effect on individuals including whether they have been informed;
- Details of how the breach is being investigated; and
- Remedial action taken to prevent future occurrence.

10 Data Sharing

Data sharing means the disclosure of data from COPNI to a third party organisation. Before disclosing personal information to another organisation, staff will ensure all sharing is lawful, fair, transparent and in line with the rights and expectations of data subjects. Data processing/sharing agreements will be put in place when required.

11 Individuals' Rights

The Data Protection Act 1998 gives individuals certain rights in respect of personal information held about them by others.

- **Right to be informed** – Individuals have the right to be informed about the collection and use of their personal data.
- **Right of access** – Individuals have the right to obtain confirmation that their data is being processed and they have the right of access to their personal data. COPNI must verify the identity of the person making a Subject Access Request using reasonable means. Information must be provided without delay and at the latest within one month of the request.
- **Right to rectification** - Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. Requests can be verbal or in writing. Responses must be made within one month. Requests for rectification can be refused in certain circumstances.
- **Right to erasure** - Individuals have the right to have personal data erased. This is also known as the right to be forgotten. Requests can be verbal or in writing. Responses must be made within one month. This right is not absolute and only applies in certain circumstances.

- **Right to restrict processing** - Individuals have the right to request the restriction or suppression of their personal data. Requests can be verbal or in writing. Responses must be made within one month. This right is not absolute and only applies in certain circumstances. When processing is restricted, you can store the data but not use it.
- **Right to data portability** - Individuals have the right to obtain and reuse their personal data for their own purposes. This allows individuals to copy, move and transfer personal data between one IT environment and another in a safe and secure way, without affecting its usability. This right is only applied to information the individual has provided to the controller.
- **Right to object** - Individuals have the right to object to processing based on legitimate interests, direct marketing and processing for the purposes of research and statistics.
- **Rights in relation to automated decision making and profiling** – Individuals have the right to prevent decisions being made about them through automated processing, including profiling.

12 Making a Subject Access Request

A Subject Access Request can be made either verbally or in writing (this includes email). The details of your request can be made to any member of staff. Any Subject Access Requests received will be coordinated by:

Data Protection Officer
Commissioner for Older People for Northern Ireland
Equality House
7-9 Shaftesbury Square
Belfast
BT2 7DP
Email: info@copni.org
Tel: [028 90890892](tel:02890890892)

When a Subject Access Request is submitted on behalf of another individual, evidence of entitlement to the information must be provided. This may include, for example, the written authority of that person or a power of attorney.

COPNI reserve the right to withhold information pursuant to Schedule 2, Part 3, section 16 of the Data Protection Act 2018 to protect the rights of other individuals.

COPNI reserve the right to withhold information pursuant to the exemption provision at Schedule 2, Part 2, section 7 of the Data Protection Act 2018.

COPNI reserve the right to decline Subject Access Requests pursuant to Article 24(5)(b) of the Data Protection Act 2018 where COPNI estimates that the costs of complying with the request would exceed the appropriate maximum as specified by the Secretary of State by regulations.

If you feel that your Subject Access Request has not been handled appropriately you have the right to complain to COPNI through our complaints procedure (a copy of this can be obtained by contacting us). You can also ask the Information Commissioner's Office to make an assessment of whether or not COPNI is complying with the Act's provisions. For more information, you can visit their website www.ico.org.uk, email casework@ico.org.uk or telephone 0303 123 1113.

13 Policy Awareness

A copy of this policy will be included within the Employee Induction Pack for all appointees. A copy of this policy will also be posted on our website, as will any subsequent revisions. On approval of changes to this policy it will be recirculated to all staff and will be discussed regularly at Team Meetings. All staff and relevant third parties are to be familiar with and comply with this policy at all times. Any breach of this Data Protection and Security Policy may result in disciplinary action being taken against staff involved in the breach.

14 Policy Review

This policy will be reviewed every two years and presented to the Commissioner or Chief Executive for approval. This policy may require review to address operational changes or new legislation. COPNI will address such matters as they arise.