DATA PROTECTION AND CONFIDENTIALITY POLICY

VERSION	1.0 draft 21/9/22
Date Equality Screened	13 February 2023
Approved by IGG	10 January 2023
Approved by EMT	22 March 2023
Approved by Business Committee	2 May 2023
Approved by Council	9 May 2023
Review Date	May 2025

CONTENTS

1. INTRODUCTION

1.1 Background

The Patient and Client Council (PCC) needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include Health and Social Care patients and clients, carers, employees (present, past 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, police, regulatory bodies and health and social care bodies).

As a public body, the PCC 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 the PCC is fundamental to how we do our business and essential to maintain the confidence of our service users, the wider public and employees.

1.2 Data Protection Principles

The PCC, 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 UK General Data Protection Regulation (UK GDPR), namely that personal information will be:

1. processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
4. accurate and, where necessary, kept up to date (accuracy);
5. 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 (storage limitation);
6. 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 (integrity and confidentiality - security)

In accordance with the seventh principle (Accountability) the PCC takes responsibility for what it does with personal data and how it complies with the six principles above. This includes ensuring that we have appropriate systems and measures in place

2. PURPOSE

The purpose of this policy is to set out:

- The PCC's commitment to data protection, ensuring that the personal data it holds is managed in accordance with UK GDPR; and
- the principles that must be observed by anyone who works for, or on behalf of, the PCC and has access to personal information.

This policy also 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.

3. SCOPE

The scope of this policy is to support the protection, control and management of personal information. The Policy covers all information within the PCC and is concerned with all information systems, electronic and non-electronic information and information systems, information in all formats and all types of media.

It applies to all services and Departments, all permanent and temporary staff, all agency staff, and as appropriate to contractors and third-party service providers acting on behalf of the PCC.

This Policy should be read alongside all PCC Information Governance policies and procedures, and in particular, the Information Governance Strategy and Framework, Records Management Policy and suite of ICT Security Policies, which deal with the security of information held by PCC and give important guidance in this respect.

4. DEFINITIONS

4.1 Personal Information

Personal data is that 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.

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

4.2 Special categories of personal information

Personal information may also include special categories of personal data, which are considered to be more sensitive and therefore require additional protections.

The UK GDPR (Article 9) defines special category data as:

- Personal data revealing **racial or ethnic origin**;
- Personal data revealing **political opinions**;
- Personal data revealing **religious or philosophical beliefs**;
- Personal data revealing **trade union membership**;
- **Genetic data**;
- **Biometric data** (where used for identification purposes);
- Data concerning **health**;
- Data concerning a person's **sex life**; and
- Data concerning a person's **sexual orientation**.

4.3 Data Controller

The 'data controller' is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

4.4 Data Processor

A 'data processor' is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of, and only on the instructions of, the data controller.

5. OBJECTIVES

The PCC is committed to following the principles for processing personal data as set out in the UK GDPR, and listed above. In order to operationalise this, the PCC will adopt the following policy objectives and associated measures:

5.1 Data Protection by Design and Default

Data protection by design means considering data protection and privacy issues upfront in everything that we do; data protection by default means only processing the data that is necessary to achieve our specific purpose. The PCC will integrate data protection into all our processing activities and business practices. This includes:

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

Appendix 1 provides further information on Data Protection Impact Assessments.

5.2 Fair and Lawful Processing

The PCC 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 relevant lawful bases set out in Article 6 of the UK GDPR and special category conditions set out in Article 9 of the UK GDPR.
- Provide transparent information on how personal information will be processed by way of a Privacy Notice/s, which will include:
    - The personal information that is processed;
    - The purposes of processing (why we need the information and what we do with it);
    - The lawful basis for processing;
    - How long we will keep the information (retention periods);
    - The rights of individuals;
    - The name and contact details for the PCC, including for the Data Protection Officer.
- Ensure the quality of personal information processed.

5.3 Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. The PCC will not disclose personal information to any third party unless it is lawful to do so in accordance with the UK GDPR and Data Protection Act 2018.

5.4 Safeguarding Information

The PCC will:

- ensure appropriate technical and organisational security measures are in place to safeguard personal information so as to prevent loss, destruction or unauthorised disclosure;
- ensure there are mechanisms in place to report breaches of the personal data;
- manage and investigate all reported data breaches appropriately.

Appendix 2 provides further information on data breach management.

5.5 Retention and Disposal

The PCC will not 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 the PCC will:

- Apply retention policies to all personal information, in line with the PCC Retention and Disposal Schedule, ‘Good Management Good Records’;
- 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 appropriate and necessary.

5.6 Uphold Individual's Rights

The PCC will ensure that the rights of the individual under UK 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
- Rights in relation to automated decision making and profiling.

Appendix 3 provides further information on the right to access, through Subject Access Requests.

6. ROLES AND RESPONSIBILITIES

6.1 Council

The PCC Council has overall responsibility to ensure compliance in all areas of information governance.

6.2 Chief Executive

The Chief Executive, as Accountable Officer, has responsibility for ensuring that sound systems of Corporate and Information Governance are in place within the PCC and to ensure compliance with legal and statutory obligations. They have ultimate responsibility for the implementation of this policy and related policies and procedures.

6.3 The Personal Data Guardian (PDG)

The PDG (Head of Operations) has responsibility for ensuring that the PCC processes satisfy the highest standards for handling personal data. Acting as the "conscience" of the organisation, the PDG actively supports work to enable information sharing where it is appropriate, and advises on options for lawful and ethical processing of information. The PDG also has a strategic role, which involves representing and championing confidentiality and information sharing requirements at senior management level.

6.4 The Senior Information Risk Owner (SIRO)

The SIRO (Head of Development and Corporate Services) is the focus for the management of information risk at Board level.

6.5 Information Asset Owners (IAO)

The IAOs are senior individuals involved in running a business area or Function within the PCC. They are accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets.

Their role includes understanding what information is held, what is added and what is removed, how information is moved, who has access to it and why, and ensure that this is recorded in the Information Asset Register, maintaining and reviewing this regularly. This includes ensuring that personal information is processed in accordance with this Data Protection Policy.

6.7 The Data Protection Officer (DPO)

The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection requirements. The DPO provides advice and recommendations on data protection, and facilitates compliance with UK GDPR. The Business Services Organisation (BSO) DPO acts as the PCC DPO, under the Service Level Agreement between the BSO and the PCC.

6.8 Managers

Managers are responsible for ensuring that this Policy and its supporting procedures, standards and guidelines are built into local processes and that there is on-going compliance with the requirements set out in these documents. They must also ensure that staff are adequately trained and apply the appropriate measures.

6.9 All Staff

It is the responsibility of all staff, whether permanent, temporary or Agency, to make themselves familiar with and comply with this Policy and all associated procedures and guidelines. They must also ensure that they complete and refresh all the mandatory information governance training.

All staff, whether permanent, temporary, seconded, Agency workers, students or volunteers should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. Failure to maintain confidentiality may lead to disciplinary action, up to and including dismissal.

6.10 Third Parties

Any third parties who are users of personal information processed by the PCC will be required to confirm and demonstrate that they will abide by the requirements of Data Protection legislation.

6.11 Information Governance Group

The PCC operates an internal Information Governance Group (IGG), comprised of the SIRO, PDG, DPO and IAOs. The IGG's role includes:

- Developing and reviewing information governance policies and procedures;
- Leading on the implementation of information governance policies and procedures across the PCC;
- Maintaining an overview of incidents affecting information governance and security;
- Promoting a good information governance culture across the PCC, disseminating information and learning across their teams.

6.12 Business Committee

The PCC Business Committee, is a Committee of the PCC Council, that has oversight of PCC information governance processes, advising the Council on the adequacy of assurances.

7. PERFORMANCE AND MONITORING COMPLIANCE

The effectiveness of this Policy will be assessed on a number of factors, including:

- compliance with the requirements of the UK GDPR and the DPA 2018;
- the management of data breaches, including near misses;
- the retention and disposal of records in accordance with Department of Health 'Good Management Good Records';
- completion of a satisfactory Information Management Assurance Checklist to the Department of Health;

8 NON-COMPLIANCE

A failure to adhere to this Policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal.

In relation to the use of ICT equipment including the use of the Internet and e-mail, 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.

Serious breaches may be reported to the PSNI, Information Commissioners Office (ICO) or other public authority for further investigation.

9 REVIEW

This Strategy and Framework will be reviewed no later than five years from approval, to ensure its continued relevance to the effective management of information governance within the PCC. However, should there be any major internal or external changes, including, but not limited to, legislative or guidance changes, it will be reviewed earlier.

Additionally, the Information Governance Improvement/Action plan will be reviewed and revised annually, ensuring that the PCC has a process of continuous improvement in place.

10. EQUALITY AND HUMAN RIGHTS SCREENING

To be completed

DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) forms part of the 'privacy by design' approach to the handling of personal information and is seen as a practical tool that will help you assess the risks in any new or revised project or process.

A DPIA must be conducted for any new project or new way of working that involves processing personal data. It helps business areas to identify and mitigate the privacy risks of the project or new way of working, and is an example of best practice, allowing you to build in openness and transparency, demonstrating compliance with data protection law as well as building trust and engagement with individuals.

The focus of any DPIA should be on 'data protection' and the measures that must be put in place to mitigate any potential risks to privacy when processing personal data. A DPIA will help you assess those risks and determine whether you need to introduce any safeguards, what these should be and how they should be put in place. This documented process will also help to provide reassurance to those whose data you plan to process

When is it appropriate to complete a DPIA?

A DPIA should be started at the **outset** of:

- any new project involving the processing of personal or sensitive data;
- making any significant change to an existing process that involves the processing of personal or sensitive data;
- a new way of gathering information (e.g. online as opposed to paper);
- a change in the way information is stored or secured (e.g. cloud storage);
- Introducing a new software system or database involving the processing of personal or sensitive data.

The DPIA should be regularly reviewed throughout the process with the final outcomes integrated back into your project plan.

The regionally agreed DPIA template should be used to guide and record the assessment. The template, and associated guidance, can be found at: https://community.sharepoint.hscni.net/sites/dpafoicomp/Reference_Docs/20230126_DPIA_v3.0.docx?Web=1

Who should complete a DPIA and who should be consulted?

Responsibility for completion of DPIA's lies with the business area introducing the new system/process and ultimately with the Information Asset Owner (IAO) responsible for that business area.

The relevant manager or Project Lead will complete the DPIA based on their knowledge of data flows, information systems and related risks.

Consultation is an important part of the DPIA process and should be built into all stages of the process. How this is conducted will depend on a number of factors such as the size and scale of the project, but may involve seeking the views and advice from internal or external sources who can provide advice based on their area of interest or expertise (e.g. ICT, Information Governance staff or external providers); or those who will be affected by the new project (e.g. staff or data subjects).

Who should approve a DPIA?

Once the draft DPIA is completed, it must be signed off by the relevant manager or Project Lead.

It will then be forwarded to the Data Protection Officer (DPO) to consider data protection compliance issues, including the 'step 5' mitigating measures, and to advise on whether the proposed data processing can proceed.

Final DPIA sign-off will be by the relevant Information Asset Owner (IAO); who will consider any DPO comment(s) and any residual risks before approving the document.

Although the aim of the DPIA is to address any data protection risks, the IAO in consultation with the relevant manager or Project lead, may also need to consider jointly or separately any other corporate or compliance risks or connected operational issues before giving approval to proceed with the new system or process.

If considering accepting any residual high risk to personal data, the Information Commissioner's Office (ICO) must be consulted before going ahead. This should first be discussed by the IAO, the Information Governance staff (Business Support Unit) and the DPO.

DATA BREACH MANAGEMENT

"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." (UK GDPR)

Examples of personal data breaches include (but are not limited to):

- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission;
- Loss of availability of personal data;
- Access by an unauthorised third party (including a member of staff who has no business need or authorisation to access that data, or an authorised member of staff who is accessing the data for reasons outside of the authorised purposes);
- Deliberate or accidental action (or inaction) by a controller or processor.

All data breaches, or suspected data breaches, MUST be reported to the DPO (either directly or through the Business Support Unit) as soon as they have been identified.

The DPO will gather the relevant information about the data breach and initiate an investigation.

The UK GDPR places a duty on all organisations to report certain personal data breaches to the Information Commissioners Office (ICO) within 72 hours of becoming aware of the breach. It is therefore essential that data breaches are reported to the DPO as soon as identified, so that the DPO can ascertain the nature of the breach and report it to the ICO if necessary.

The DPO is responsible for advising on whether the individuals whose data has been breached need to be informed. (ie where an individual's rights and freedoms are at a high risk of being adversely affected, they must be informed without undue delay.)

The DPO is responsible for leading the investigation into the data breach, with the assistance of the PCC business support unit. This may include the establishment of an incident management team. All staff must co-operate with any such investigation.

The PDG and the Chief Executive should be made aware of any data breach. Reports, including the outcome of investigations and any recommendations on actions to improve data protection, will also be made to the IGG and the PCC Business Committee, and where appropriate to the PCC Council.

A record will be held of all personal data breaches, regardless of whether they are notified to the ICO. Disclosure of personal data breaches should be included in the PCC Annual Report, as directed by the relevant guidance on completion of the Annual Report.

SUBJECT ACCESS REQUESTS

UK GDPR gives individual's the right to have access to their personal data. The ICO provides the following summary:

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a Subject Access Request (SAR).
- Individuals can make a SAR verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person if appropriate consent has been provided.
- SARs should be responded to without delay and within one month of request. This can however be extended by a further two months if the request is complex or if a number of requests have been received from the individual.
- A reasonable search must be performed for the requested information.
- The information must be provided in an accessible, concise and intelligible format.
- The information must be disclosed securely.
- The request to provide information can only be refused if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

While a SAR may be received by any member of staff across the PCC, it must be responded to in the appropriate and approved manner, in line with the agreed PCC SAR procedures as found on the PCC Sharepoint:

https://pcc.sharepoint.hscni.net/sites/pcc/PaP/PCC%20Staff%20Handbook%20-%20Policies,%20Processes%20and%20Procedures/Processes%20(Employee%20Responsibilities)/Misc%20Processes%20and%20Guidance%20Notes/Internal%20procedure%20for%20Handling%20FOIs%20and%20SARs%20March%202023.docx?Web=1

All SARs (or potential SARs) should therefore be forwarded to PCC Business Support as soon as received, to be dealt with in accordance with the agreed processes.

All staff must co-operate with the PCC Business Support Unit to carry out the necessary searches for requested personal information.