Policy Title	**DATA PROTECTION POLICY**
Version	V1
Policy Summary	The policy details the principles and processes by which the Office of the Civil Service Commissioners will protect personal data with regards to its collection, use and storage.
Source / Author(s)	Office of Civil Service Commissioners.
Date of Equality Screening	8/7/2019
Date of Commissioner Approval	26/6/2019
Implementation Date	8/7/2019
Last Review Date	NA
Next Review Date	7/7/2022
Officer Responsible for Review	Secretary
Any Other Information	This policy can be provided in alternative formats if required in relation to language or disability.

Revision History

Date	Changes Made	Version
		V1

Data Protection Policy

Policy Summary	The policy details the principles and processes by which the Office of the Civil Service Commissioners (OCSC) will protect personal data with regards to its collection, use and storage.
Requirement for policy	Policy is required to ensure the OCSC meets its obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA), which came into force on 25 May 2018.
Relevant Legislation	The OCSC must comply with all relevant statutory UK and European Union legislation that have links to the GDPR and DPA. These include, but are not limited to, those listed in Appendix 1.
Linkage with other Policies and Procedures	This policy supports, and is supported by, other OCSC policies, standards and procedures. These include, but are not limited to, those listed in Appendix 1.
The Data Protection Act 1998	All references to the Data Protection Act 1998 within OCSC documentation, including existing polices, should now be read as references to the GDPR and DPA 18.

Definitions

A range of definitions are provided below, however, any term relating to data protection not included within this section will be defined in line with Article 4 of the GDPR, and relevant supplementary provisions of the DPA.

'**Personal Data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'**Special Categories of personal data'** means any information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

'**Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**Commissioners**' means those individuals appointed by Royal Warrant to exercise the powers and responsibilities set out in the Civil Service Commissioners (NI) Order 1999;

'**Restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

'**Profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'**Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

'**Filing system'** means any structured set of personal data which are accessible according to specific criteria, held electronically or in hard copy whether centralised, decentralised or dispersed on a functional or geographical basis;

'**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

'**Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'**Third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'**Personal data breach**' The Article 29 Working Party ("WP29") defined three types of personal data breaches following the three well-known information security principles:

- "Confidentiality breach" – where there is an unauthorised or accidental disclosure of, or access to, personal data, which is about getting knowledge of personal data by an entity not entitled to this knowledge;
- "Availability breach" – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which is about losing control of access to personal data, or inappropriate deletion of personal data; and
- "Integrity breach" – where there is an unauthorised or accidental alteration of personal data, which is about inappropriate modifications of personal data.

'**Biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

'**Elected Representatives'** refers to Councillors, MLAs, MPs, MEPs and any other Government Minister or elected representative.

Who does this policy apply to?

The obligations contained in this Policy apply equally to:

- all OCSC staff, including those on secondment or agency workers;
- Commissioners working on OCSC business;
- Partners and other third parties, including contractors, volunteers, agencies and any other organisation(s) processing personal information on behalf of the OCSC are bound by the practices established in this policy and the terms of the agreement or contract with the OCSC.

What does this apply to?

This policy applies in all circumstances in which personal data is processed by the OCSC, or on its behalf, either manually or automatically. This will apply to:

- Information that is processed automatically;
- Information that is recorded with the intention that it should be processed automatically;
- Information that is recorded as part of a relevant filing system or with the intention of being part of such a system;
- Information that does not fall within the above three categories but which forms part of an accessible record;
- Information which is recorded and held by the OCSC which does not fall within the above four categories.

This means that the handling (processing) of any personal data (including data in both paper/hard or electronic form) from which an individual (data subject) can be identified, either directly or indirectly is covered by this policy from the time the information is collected through to its destruction.

Data Protection Principles

The data protection principles set out the main responsibilities to which the OCSC will adhere when processing personal information. Personal information shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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.

Legal basis for processing

Processing of all personal data by the OCSC must be grounded on at least one legal basis for processing:

1. **Consent**: the individual has given clear consent for the processing of their personal data for a specific purpose.
2. **Contract**: the processing is necessary for a contract the OCSC has with an individual or because an individual has asked the OCSC to take specific steps before entering into a contract.
3. **Legal obligation**: the processing is necessary for the OCSC to comply with the law (not including contractual obligations).
4. **Vital interests**: the processing is necessary to protect a data subject's life.
5. **Public task**: the processing is necessary for the OCSC to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
6. **Legitimate interests**: the processing is necessary for the OCSC's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legal basis for processing special category data

The processing of special category data is prohibited unless at least one of the following legal basis for processing applies:

1. **Consent**: the individual has given explicit consent for the processing of their personal data for a specific purpose.
2. **Employment and Social Security**: processing is necessary for the purposes of carrying out obligations in the fields of employment, social security and social protection law.
3. **Vital interests**: the processing is necessary to protect a data subject's life.
4. **Not-for-Profit Bodies:** processing is carried out for the members, and in the course of the legitimate activities of, a foundation, association or trade union.
5. **Manifestly Public**: processing relates to personal data which are manifestly made public by the data subject.
6. **Legal Claims:** processing is necessary for the establishment, exercise or defense of legal claims.
7. **Substantial Public Interest:** processing is necessary for reasons of substantial public interest.
8. **Medicine:** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis or health and social care.
9. **Public Health:** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.
10. **Archiving:** processing is necessary for archiving purposes in the public interest, scientific, historical or statistical purposes.

Privacy Statement

The OCSC will take all reasonable steps to ensure that data is obtained and processed fairly and that individuals are aware of the processing activities which the data will be subject to (this applies to data collected in paper or electronic format).

If the OCSC collects personal data directly from data subjects, it will inform them about:

a) The purpose or purposes for which it intends to process that personal data and the lawful basis for processing it;
b) The names or types of third parties, if any, with which information will be shared or to which the OCSC will disclose that personal data;
c) The means, if any, with which data subjects can limit OCSC use and disclosure of their personal data; and
d) Contact details of the Data Protection Officer.

In order to do this, the OCSC will provide a Privacy Statement at the point at which data is collected from a data subject. If data is collected verbally whether over the phone or in person, the data subject will be directed to the Privacy Statement.

The Privacy Statement (Appendix 2) provides further information on data subjects rights and OCSC's practices and procedures. This policy is available from the OCSC's website at: https://www.nicscommissioners.org

---

Data Protection fee

The OCSC will pay all fees, relating to its responsibilities as a data controller only, as required under section 2 of the Data Protection (Charges and Information) Regulations 2018.

Clear Desk Policy

All staff must adhere to the secure desk policy which is an important measure to ensure that documents containing personal data are removed from a user's workspace and locked away when the items are not in use. The practice also reduces the risk of security breaches occurring.

In order to adhere to the clear desk policy, all staff should ensure they apply the following principles:

- Computer/laptop screens should be locked when the workspace is left unoccupied even temporarily;
- Computers must be shut completely down at the end of the working day;
- Laptops/mobile devices should be locked away in a secure cabinet or be removed safely from the premises for remote working;
- Any external storage devices such as CD/DVD-ROM or USB drives should be stored securely or be removed safely from the premises for remote working;
- Combination codes and keys used to access personal data must not be left at an unattended desk;
- Passwords must not be left on sticky notes posted on or under a computer, nor should they be left written down in an open, accessible location;
- All printers should be cleared of papers as soon after they are printed as possible.

Documents containing personal information, which are likely to be needed by other members of staff, should be stored in shared, lockable filing cabinets.

In so far as is reasonably practicable, any documents containing personal information on the desks or workstation, or open on the computer screen, should not visible to visitors, members of the public or colleagues who are not authorised to see them.

Data Sharing

The OCSC will ensure that any data sharing arrangements are legitimate and comply with the principles of the GDPR and DPA 18 and therefore adopt the ICO's Data Sharing Code of Practice (and any successor Code of Practice) as the basis for its own data sharing arrangements.

The OCSC will primarily utilise two types of data sharing:

- As part of a systematic and routine process where personal data is shared on the basis of a lawful processing condition (for example, information shared with NICS HR or HR Connect); or

- In exceptional circumstances, the OCSC may be required to share or request from a third party, personal data on the basis of a lawful processing condition (for example, to protect the vital interests of a data subject);

The Secretary must be notified and consulted before the OCSC enters into any data sharing arrangement to ensure that all relevant matters and practices have been taken into consideration, such as the completion of a Data Protection Impact Assessment.

Data Protection Impact Assessment & Screening

The OCSC will conduct a screening exercise to identify data protection implications and, if necessary, conduct a Data Protection Impact Assessment (DPIA) (appendix 3):

- before the introduction of a new processing activity or activities (including the introduction of new policies, technologies or operational procedures); or
- before a change is made to an existing processing activity or activities (including a change to existing policies, technologies or operational procedures);

and

- if the introduction or change in processing activity or activities is likely to result in a high risk to individuals' interests, including, physical, material or non-material damage.

This includes where processing may give rise to:

- discrimination;
- identity theft or fraud;
- financial loss;
- damage to reputation;
- loss of confidentiality of personal data protected by professional secrecy;
- unauthorised reversal of pseudonymisation;
- any other significant economic or social disadvantage; or
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.

A DPIA will also be necessary where:

- automated processing is used to make decisions which produce legal effects concerning the data subject or significantly affect the data subject;
- there is large scale processing of special category data or data relating to criminal convictions or offences; or

Conducting a DPIA in the above circumstances is mandatory and must be completed using the form in Appendix 3. The Secretary should sign off on all DPIAs.

Data Sharing Register

The Secretariat will maintain a central register of all data sharing arrangements; and contracts with third party processors.

This will include:

- The title of the contract or agreement, and the parties to it;
- A description of the data to be shared or transferred
- Details of the processing activities, including basis for processing;
- Process for the destruction or retention of that information;
- Details of procedures undertaken by each organisation to facilitate the protection, processing and destruction of information which has been shared;
- Contact details for key individuals within each respective party to the agreement or contact; and
- The date the agreement or contract is effective, terminates and, if applicable, is reviewed.

Destruction of Personal Data

Personal data held by the OCSC shall be destroyed in line with the OCSC's Retention and Disposal Schedule.

Personal data held on behalf of the OCSC by a third party processor will be destroyed in line with the terms of that contract or agreement.

All destruction of personal data is subject to the exercise of the right to erasure.

Data Subject Rights

The GDPR provides the following rights for individuals whose personal data is being processed by the OCSC:

- The right to be informed - individuals have the right to be informed about the collection and use of their personal data;
- The right of access – individuals have the right to obtain confirmation that the personal data is being processed and have access to it;
- The right to rectification - a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete;
- The right to erasure - a right for individuals to have personal data erased;
- The right to restrict processing - individuals have the right to request the restriction or suppression of their personal data;
- The right to data portability- allows individuals to obtain and reuse their personal data for their own purposes across different services;
- The right to object – allows individuals to object to processing

based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

Queries relating to any of the above rights should be made directly to the Secretariat:

Post:
Office of the Civil Service Commissioners for Northern Ireland
Room 105
Stormont House
Stormont Estate
Belfast
BT4 3SH

Telephone: 028 9052 3594
Email: info@commissioners.org

Queries received by a third party processor or partner in a data sharing agreement shall be forwarded to the Secretary at the details above.

The OCSC will acknowledge receipt of all communications concerning data subject rights. Matters relating to those rights will be responded to as soon as possible but no later than one calendar month from the date communication is received.

The OCSC will request photographic ID as proof of identity in all circumstances where the identity of the individual is required to be confirmed.

Data Subject Rights - Review

If an individual is unhappy with the way in which the Secretariat has dealt with matters relating to their data subject rights request then they may request that the decision, or handling of the matter, be reviewed by the Secretary within one calendar month of a response being issued by the Secretariat. An individual can contact the Information Commissioner's Office (ICO) at any time if they are unhappy with the review process.

ICO Office – Northern Ireland
3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

Personal Data Breaches

The Article 29 Working Party ("WP29") defined three types of personal data breaches following the three well-known information security principles:

- "Confidentiality breach" – where there is an unauthorised or accidental disclosure of, or access to, personal data, which is about getting knowledge of personal data by an entity not entitled to this knowledge;
- "Availability breach" – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which is about losing control of access to personal data, or inappropriate deletion of personal data; and
- "Integrity breach" – where there is an unauthorised or accidental alteration of personal data, which is about inappropriate modifications of personal data.

All personal data breaches, either as a result of OCSC action or those of a third party processor, must be notified to the Secretary as soon as possible after the breach has taken place or been identified. The breach notification process is detailed in Appendix 4.

The OCSC will maintain a Data Breach Register which will contain the following information:

- Details of each data breach including the date, nature, specific details of the information released and details of when the breach was notified;
- Details of any remedial action taken, or action taken to minimise the impact of the data breach;
- Whether and when the NIO has been notified and details of considerations which informed that decision;
- Whether the ICO has been notified and details of considerations which informed that decision;
- Whether the data subject has been notified; and
- In the context of the breach, any other information which it is considered necessary to record.

The NIO's Data Protection Officer and Senior Information Responsible Officer should be notified of all data breaches without undue delay. The NIO's Data Protection Officer, in consultation with Senior NIO Officials and the Secretary, will determine if a suspected breach constitutes a sufficient risk to the rights and freedoms of natural persons to require notification to the ICO. Any notification to the ICO must take place not later than within 72 hours of the breach occurring or the OCSC becoming aware of it.

Commissioners will be notified of any breach reported to the ICO.

Circumstances relating to a personal data breach, which was the established fault of a third party processor or partner in a data sharing arrangement, may, dependent on the terms of that agreement or contract, trigger a review of that arrangement.

Disclosure of Personal Information to Third Parties	Personal information will only be disclosed to other third parties with the express written permission of the individual to whom the information belongs.
Disclosure of Personal Information to Statutory Law Enforce-ment Agencies	The Data Protection Act includes exemptions which allow personal data to be disclosed to statutory law enforcement agencies without the consent of the individual who is the subject of the data, and regardless of the purpose for which the data where originally gathered. In particular, personal data may be released in relation to those exemptions detailed within Schedule 2 of the DPA. Guidance on disclosing information to statutory law enforcement agencies can be found in Appendix 5.
Demonstration of Compliance	In order to demonstrate compliance with data protection laws, the OCSC will complete and return the NIO Information Assurance Statements and quarterly returns as required. Every six months the OCSC will complete the GDPR Compliance Checklist (Appendix 6), and will document and retain the evidence to demonstrate that personal data is being processed in accordance with data protection legislation. A section on GDPR compliance will be included in the Annual Report.

Publication and Alternative Formats

This document will be made publicly available through the OCSC's website and available in a range of alternative formats on request by contacting:

Post:
Office of the Civil Service Commissioners for Northern Ireland
Room 105
Stormont House
Stormont Estate
Belfast
BT4 3SH

Telephone: 028 9052 3594
Email: info@commissioners.org

Appendix 1 – Relevant Legislation & Policies

Relevant Legislation

The OCSC must comply with all relevant statutory UK and European Union legislation that have links to the GDPR and Data Protection Act 2018 these include, but are not limited to:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Common law Duty of Confidence
- Public Records Act (Northern Ireland) 1923
- Regulation of Investigatory Powers Act 2000
- Criminal Justice and Immigration Act 2008
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Data Protection (Charges and Information) Regulations 2018
- Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002.

Relevant Policies

This policy should be read, when necessary, in conjunction with, but not limited to, the following OCSC and NIO policies:

- Information Security Policy(NIO)
- Information Management Policy (NIO)
- Records Management Policy (draft)
- Retention and Disposal Schedule.

Appendix 2 – Privacy Statement

OFFICE OF THE CIVIL SERVICE COMMISSIONERS FOR NORTHERN IRELAND PRIVACY NOTICE

The Office of the Civil Service Commissioners for Northern Ireland (OCSC) is the data controller for the personal data processed on individuals in the undertaking of Commissioners' statutory duties and users of our website.

Data Controller: Office of the Civil Service Commissioners for Northern Ireland
Address: Room 105
Stormont House
Stormont Estate
Belfast
BT4 3SH
Telephone: 028 9052 3594
Email: info@commissioners.org

Data Protection Officer: Lloyd Ryan (NIO)
Telephone: 028 9076 5197
Email: foi@nio.org.uk

Why are you processing my personal information?

Commissioners have a statutory responsibility for ensuring that appointments to the Northern Ireland Civil Service (NICS) are made on merit on the basis of fair and open competition. Commissioners also have a statutory role which allows them to hear appeals under the NICS Code of Ethics. The vast majority of personal data processed by OCSC relates to the exercise of the powers and responsibilities set out in the Civil Service Commissioners (Northern Ireland) Order 1999.

In broad terms, this legislation allows the OCSC to process data in relation to appointments to the NICS; to maintain the principle of selection on merit on the basis of fair and open competition in relation to selection for appointment to the NICS; and to consider and determine appeals made by existing civil servants under the NICS Code of Ethics.

We may hold your personal information to allow us to deal with your query or concern.

Where we are relying on your consent to process your personal data we will make this clear.

Where do you get my personal data from?

We receive personal data from:

- HR Connect on behalf of NICS as part of the procedure for appointments made through open competition to posts in the Senior Civil Service (SCS);

The 4-Stage Authorisation Process for appointments to the SCS sets out the information and the assurances which must be checked by HR Connect or departments and agencies and provided to the OCSC to ensure that the Merit Principle is upheld throughout the NICS recruitment process;

- NICS departments and agencies and NICS HR in relation to requests for Commissioners' approval of appointments made by way of exception to the merit principle. The circumstances of appointments to be made other than in accordance with the Merit Principle are described in the Commissioners' Recruitment Code;

- NICS departments and agencies and NICS HR in undertaking statutory audit functions to monitor the application of merit in NICS recruitment and selection processes; and

- Civil servants or members of the public who provide personal information which may include the personal data of others involved in a concern or query being raised to Commissioners.

You will need to provide your personal information if you are an existing civil servant bringing an appeal under the NICS Code of Ethics to Commissioners. We may contact the NICS departments and agencies and NICS HR with your personal information, and the NICS may provide personal information in relation to the Commissioners' consideration / determination of a concern raised under the NICS Code of Ethics.

You may need to provide your personal information if you contact us or if you wish Commissioners to consider a concern / an issue raised by you which falls under our statutory role.

Our website collects data in relation to your visit to our website and does not identify you personally. It provides us with information including your Internet Protocol (IP) address, the pages you visited, when you visited and how long you visited the website for. We use this information to analyse usage of the website.

Do you share my personal data with anyone else?

To deliver our statutory role we may need to share your information with:

- the Northern Ireland Civil Service (NICS) departments and agencies, including NICS HR;
- HR Connect;
- Crown Solicitor's Office;
- Professional advisors, consultants or contractors working on OCSC's behalf, who are subject to obligations of confidentiality; and
- our sponsor Department NIO.

As required by law, we may disclose information to government bodies and law enforcement agencies for their enforcement purposes.

Do you transfer my personal data to other countries?

The OCSC does not transfer personal information overseas.

How long do you keep my personal data?

We will only retain your personal data for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable laws or regulations, and in line with our Retention and Disposal Schedule.

What rights do I have?

You have rights as an individual which you can exercise in relation to the information we process about you. To learn more about these rights, please visit the ICO website.

You have:

- the right to be informed about the collection and use of your personal data;
- the right to access the data we hold on you;
- the right to have your data rectified if it is inaccurate or incomplete;
- the right to have your personal data erased in specific circumstances;
- the right to have your data restricted or blocked from processing in specific circumstances;
- the right to data portability in specific circumstances;
- the right to object to processing of your personal data; and
- rights in relation to automated decision making and profiling.

How do I exercise my rights or complain if I am not happy?

If you wish to exercise any of your rights or if you are unhappy with any aspect of this privacy notice regarding the processing of your personal data, please contact the Data Protection Officer by sending an email to foi@nio.org.uk or write to:

Data Protection Officer
Stormont House
Stormont Estate
Belfast
BT4 3SH

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at:

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

Tel: 0303 123 1113
Email: casework@ico.org.uk
htpps://ico.org.uk/global/contact-us/

Changes to this Privacy Notice

We keep our Privacy Notice under regular review. This Privacy Notice was last published in May 2018.

Data Protection Screening and Impact Assessment Form

Title of Policy/Operation Change	

Please Indicate which category the activity specified in Section relates to				
New ☐	Policy ☐	Strategy ☐	Plan ☐	Service Operation ☐
Revised ☐	Policy ☐	Strategy ☐	Plan ☐	Service Operation ☐

1. Is the introduction or change of this policy or processing activity likely to result in a high risk to individuals' interests, including physical, material or non-material damage?
Yes ☐ Please give reasons below (continue to Q2) No ☐ Please give reasons below (continue to Q9)

2. 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)*

3a. 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 the data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?*

3b. 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?)*

3c. 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?)*

3d. 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 the OCSC, and more broadly?)*

4. Consultation. *(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 your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?)*

5. Necessity and Proportionality. ***(****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 minimalisation? 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?)*

6. Identify and assess risk.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm (remote, possible or probable).	Severity of harm (Minimal, significant or severe).	Overall risk (low, medium or high).

7. Identify measures to reduce Risk.

(Identify additional measures you can take to reduce or eliminate risks identified as medium or high risk in step 5)

Risk	Options to reduce to eliminate risk	Effect on risk (eliminated, reduced or accepted)	Residual risk (low, medium or high)	Measure approved (yes/no)

8. Sign off and record outcomes.

Item	Name/Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If accepting any residual risk, consult ICO before going ahead.
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
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 be kept under review by:		The DPO should also review ongoing compliance with DPIA.

9. Data Protection Screening and Impact Assessment completed by:
Name:
Title:
Date:
Signature:

Director/Head of Service decision approved by:
Name:
Title:
Date:
Signature:

Appendix 4 – Personal Data Breach Notification

Personal Data Breach Examples

- An email sent to the wrong, unintended or unauthorised recipient;
- The wrong document being attached to an email;
- Data downloaded on to a memory stick and then being mislaid;
- An unnecessary level of data being downloaded on to a disc and lost in the post;
- A laptop or iPad containing personal data being stolen from a car; or
- A computer being accessed by an unauthorised party.

Impact of Personal Data Breach

The effect of a security breach on the OCSC can range from bad publicity and a loss of public confidence to a significant financial penalty being levied.

Impacts of a personal data breach will be categorised by the extent to which it breaches one or multiple of these breach factors:

- Confidentiality;
- Integrity;
- Availability; and
- Accountability

Incident Reporting

Any actual or suspected loss of personal data must be reported to the Secretary by submitting a completed Incident Report Form within 24 hours of the breach occurring or becoming aware of it.

All breaches will be recorded in the OCSC's Data Security Breach Register.

Upon becoming aware of a breach the following actions should be taken:

Internal Breach	External Breach (Third Party)
Employees must report immediately to their line manager, any suspected or actual loss of personal data held or any complaints received from any source regarding suspected or actual loss. The line manager must then advise the Secretary.	Third parties processing information on the OCSC's behalf, or processing in joint controller relationship with the OCSC, must report immediately to their key contact within the OCSC, any suspected or actual loss of personal data held or any complaints received from any source regarding suspected or actual loss.

Commissioners should report any suspected or actual loss of personal data held or any complaints received from any source regarding suspected or actual loss to the Secretary.	The key contact must then contact the Secretary.
Upon becoming aware of a breach, employees should take all necessary actions to retrieve lost data and/or secure data and/or systems against further loss or complaint.	Upon becoming aware of a breach, third parties should take all necessary actions to retrieve lost data and/or secure data and/or systems against further loss or complaint.
The Secretary will work with the Commissioners, Secretariat and/or third parties to ensure all necessary actions are taken to retrieve lost data and/or secure data and/or systems against further loss or complaint. This may include, but is not limited to: - Investigating, or nominating an officer with appropriate knowledge and technical expertise, to investigate the details of the data loss; - Audit operational practices; and - Assist with the review of relevant policies. Loss relating to mobile devices or other OCSC technology will be reported to IT Assist.	
The Secretary will report the breach to the NIO's Senior Information Responsible Officer (SIRO) and Data Protection Officer.	
The NIO's Data Protection Officer, in consultation with Senior NIO Officials and the Secretary, will determine if a suspected breach constitutes a sufficient risk to the rights and freedoms of natural persons to require notification to the ICO. If notification is required, it will be done no later than 72 hours of a breach occurring or after having become aware of it. Commissioners will be notified of any breach reported to the ICO.	

Severity

The severity of an incident will be dependent on the incident and matters relating to it, for example the content of information lost, circumstances surrounding the loss and number of individuals concerned.

All incidents will be considered on their own merits, but this table attempts to provide examples of personal data breaches and the how they would be considered.

Incident Type	Breach of (confidentiality, integrity, availability & Accountability)	Severity
Information sent to an unauthorised recipient(s) containing confidential and sensitive personal information (whether Internal or External).	Integrity/Confidentiality.	Major.
Loss and theft of equipment containing confidential and/or sensitive personal information where equipment has no encryption software installed.	Availability/ Confidentiality.	Major.
Incident Type	**Breach of (Confidentiality, Integrity, Availability & Accountability)**	**Severity**
Passwords written down leading to unauthorised access.	Integrity/ Confidentiality/ Availability & Accountability.	Moderate/ Major depending on the type of information and system and impact of the incident.
Loss or theft of equipment containing no confidential and/or personal information.	Availability.	Minor/ Moderate.
Information sent to the wrong recipient (internally), disclosing information that is neither confidential not personal.	Integrity.	Minor.

CIVIL SERVICE COMMISSIONERS FOR NORTHERN IRELAND

Data Breach Incident Report Form

Date/ time of breach:
Date Line Manager notified:
Provide details of the nature of the personal data breach including: - What has happened? - How was the incident identified? - What format was the information? (if electronic, was it encrypted?) - What personal data was within the information?
Provide details of the categories and approximate number of personal data records concerned:
Provide a description of the likely consequences of the personal data breach:

Provide a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects:
Completed by: **Name:** **Date:** **Signature:**
Line Manager comments:

Data Impact Assessment

1.	Was any data lost or compromised in the incident?	Yes/No
2.	Was personal data lost or compromised?	Yes/No
3.	If yes, was sensitive personal data compromised?	Yes/No
4.	What is the number of people whose data was affected by the incident?	
5.	Is the data breach likely to result in a high risk to the individual/individuals?	Yes/No
7.	Is there a risk that the incident could lead to damage to individuals eg. via identity theft/ fraud?	Yes/No
8.	Could the incident damage an individual's reputation, or cause hurt, distress or humiliation eg. loss of medical records, disciplinary records etc.?	Yes/No
9.	Can the incident have a serious impact on the OCSC's reputation?	Yes/No
10.	Has any similar incident happened before?	Yes/No
12.	If this incident involves the loss or theft of equipment please confirm that it IT Assist are aware of the incident?	Yes/No

DPO comments:

Would the disclosed information be classed as personal data?

How many people could be affected?

How many records could be involved?

What type of data has been breached?

Was any of the information sensitive?

Was the information disclosed accidentally/ was there a legitimate reason for sharing this information?

Should consideration have been given to notify the data subjects of the disclosure beforehand?

Are you content that the measures taken to mitigate any possible adverse effects are sufficient?

Are any further measures required?

Refer to ICO: Y/N

Reason for decision:

Any further action taken:

Appendix 5 – Disclosure of personal information to law enforcement agencies

Disclosure to PSNI

The Police Service of Northern Ireland (PSNI) has a standard form (Form 81) for requesting personal data. The form should certify that the information is required for an investigation concerning national security, the prevention or detection of crime and/or the apprehension or prosecution of offenders.

This form should be signed by the PSNI Investigating Officer and must be authorised by a senior officer.

Personal information held by the OCSC should only be disclosed to the PSNI on production of a Form 81. The OCSC considers it reasonable, however, not to request the submission of a Form 81 where the OCSC is seeking the PSNI to investigate a crime/take law enforcement action on its behalf.

Disclosure to other Law Enforce-ment Agencies

Other law enforcement agencies may not use standard forms. However, any request should:

- Be in writing, on headed paper, and signed by an authorised officer of that agency.
- Describe the nature of the information which is required.
- Describe the nature of the investigation.
- Citing relevant statutory or legal authority to obtain the information.
- Certify that the information is necessary for the investigation.

Refusal & Review

The OCSC may refuse to disclose requested information if it is not satisfied that sufficient information has been provided by the requesting body, forms are not completed or for any other reason it considers reasonable and appropriate to ensure compliance with its own statutory responsibilities.

In cases of refusal of disclosure, the OCSC will explain to the requestor the reasons for withholding the information.

If the OCSC determines that it has insufficient information, the requesting body will be invited to provide further information in support of its request. The OCSC will review its decision in light of any additional information provided by the requesting body.

Appendix 6

General Data Protection Regulation (GDPR) & Data Protection Act 2018
OCSC GDPR Compliance Checklist

Date:	**Completed by:**

SECTION 1 Does the OCSC hold any personal data as defined by the ICO?

(*Please tick appropriate box below*)

☐ **No** – Complete section 2 and sign section 4

☐ **Yes** – Complete sections 2 & 3 and sign section 4

Please complete the questions below and tick the relevant box to determine if the OCSC is **fully compliant** or **not fully compliant**. Please explain in the comments section what action is required and the timescales involved for the OCSC to achieve full compliance.

If you have ticked a box stating **fully compliant**, please provide evidence of OCSC compliance. This evidence could include a relevant HP Records Manager (HPRM) reference number, records of DPA training/awareness sessions, team brief updates on DPA, Commissioner meetings where the Data Protection Act was an agenda item etc.

If you have ticked a box stating **not fully compliant**. Please explain in the comments section what action is required and the timescales involved for the branch to achieve compliance.

	Area of Compliance	**Fully Compliant**	**Not Fully Compliant**	**Provide evidence/detail of level of compliance**
SECTION 2				
1)	All staff in the OCSC have completed the GDPR Awareness e-learning training	☐	☐	
2)	All Commissioners have completed the GDPR Awareness e-learning training			

Comments: **We are aware that there are technical issues receiving accurate data from NICSHR. Please provide evidence dates of completion, where possible.**				
3)	All Commissioners and staff have been made aware of the OCSC Data Protection Policy and other data protection guidance **within the last 6 months.**	☐	☐	
Comments: **Provide <u>evidence</u> of occasions on which awareness was raised (emails to staff, discussions at team briefs etc) – HPRM link required.**				
4)	All staff have a data protection related objective included in their Personal Performance Agreements.	☐	☐	
Comments: **Provide assurance that this is included in all staff PPAs – HPRM link or other evidence required (e.g. emails issued to staff, record of discussion during team brief etc, assurances given by line manager(s) to IAO).**				
SECTION 3				
5)	All holdings of personal data, and the lawful basis for processing, have been identified and documented within the OCSC Information Asset Register.	☐	☐	
Comments: **Provide evidence of checking process (e.g. screenshot taken and placed in HPRM as evidence, confirmation email to BAIM)**				
6)	All privacy information (i.e. Privacy Notices) provided to data subjects is accurate and relevant to the personal data processing	☐	☐	

Comments: **Provide evidence of checking process (e.g. link to online privacy information, link to HPRM)**				
7)	Operational procedures are in place for processing personal data, and are provided and known to all staff	☐	☐	
Comments: **Provide HPRM links to branch procedures for processing personal data.**				
8)	Access to personal data is limited to staff with a strict need to know, and appropriate organisational and technical security measures are in place.	☐	☐	
Comments: **Provide details of how access controls are applied and any review processes in place (e.g. instructions for staff and when circulated). Provide evidence of security measures on personal data e.g. clear desk checks, locking up procedures, escorting visitors on premises, accreditation status of systems etc.**				
9)	Where appropriate, all personal data held is accurate and up to date.	☐	☐	
Comments: **Are there procedures in place to update personal details, for example, when the data subject advises of a change of address etc? Is there an annual exercise to update data? HPRM link to procedures and any other evidence is required.**				
10)	When no longer required for business purposes, personal information is destroyed securely in line with OCSC retention and disposal schedules.	☐	☐	
Comments: **Provide evidence of file reviews. What processes are in place to delete information from IT systems?**				
11)	Staff and Commissioners are aware of the requirement to report all data incidents immediately in line with the OCSC Data Breach protocol.	☐	☐	

Comments: **Provide evidence of staff awareness of plan (e.g. HPRM link to team brief, emails etc). Provide evidence of occasions on which incidents have been reported.**				
12)	Data sharing agreements are in place in all cases where personal data is shared with other data controllers (Government departments, agencies or third parties)	☐	☐	
Comments: **Provide links to data sharing agreements completed within the last six months. Provide evidence of reviews carried out on existing agreements. Provide evidence of instructions to staff to ensure data is shared in line with agreements.**				
13)	GDPR compliant contracts or MOUs are in place in all cases where personal data is shared with data processors in line with the OCSC Data Protection policy.	☐	☐	
Comments: **Provide evidence on reviews carried out on existing contracts and MOUs to make them GDPR compliant, and include actual or target date for completion. Provide evidence of instructions to staff to ensure data is shared in line with contracts and MOUs.**				
14)	Data Protection Impact Assessments (DPIAs) are considered and are completed/in progress for all new projects/systems/ processes/policies where personal data is used.	☐	☐	
Comments: **A DPIA <u>must</u> be carried out before the implementation of any high or medium risk processing of personal data, e.g. new or upgraded IT system, new policy, project, taking on a new function, any restructuring, reorganisation, office move, changes to an existing work process, data sharing initiatives, outsourcing etc. Provide evidence of DPIAs completed within the last six months. Provide evidence of DPIAs in progress.**				

SECTION 4 (*to be completed in all cases*)	
Information Asset Owner (please print):	**Date:**
Signature:	