

Title of Report:	Data Sharing Agreement – Civil Service Pensions
Committee Report Submitted To:	Corporate Policy and Resources Committee
Date of Meeting:	27 April 2021
For Decision or For Information	For decision

Linkage to Council Strategy (2021-25)	
Strategic Theme	All themes
Outcome	The Council will continuously examine and introduce ways to provide services in more accessible and efficient ways
Lead Officer	Chief Finance Officer

Budgetary Considerations	
Cost of Proposal	
Included in Current Year Estimates	YES/NO
Capital/Revenue	Revenue
Code	
Staffing Costs	Payroll time implementing

Screening Requirements	Required for new or revised Policies, Plans, Strategies or Service Delivery Proposals.		
Section 75 Screening	Screening Completed:	Yes/No	Date:
	EQIA Required and Completed:	Yes/No	Date:
Rural Needs Assessment (RNA)	Screening Completed	Yes/No	Date:
	RNA Required and Completed:	Yes/No	Date:
Data Protection Impact Assessment (DPIA)	Screening Completed:	Yes/No	Date:
	DPIA Required and Completed:	Yes/No	Date:

1.0 Purpose of Report

- 1.1 Staff who have transferred into Council at 1 April 2015 continue to have their pensions administered by Civil Service Pensions (CSP).

2.0 Detail

- 2.1 Under Data Protection legislation the necessary sharing of information between Council needs to be done in a controlled manner and to this end the attached proposed data sharing agreement has been put forward by CSP. This agreement sets out the parameters on which data will be shared, how it is to be shared, who is responsible for the data, how the data can be used, how the data is to be stored and how it is to be disposed of or returned upon termination of the agreement.

3.0 Recommendation

- 3.1 **It is recommended** that Council approve the signing of the data sharing agreement with Civil Service Pensions.



DATA SHARING AGREEMENT

between

***Civil Service Pensions
(Department of Finance)***

and

1. Parties to the Data Sharing Agreement

<p>Civil Service Pensions Department of Finance</p> <p>Waterside House Room 136 75 Duke Street Londonderry BT47 6FP Tel No: 028 71321202</p> <p>Email: Margaret.Coyle@finance-ni.gov.uk</p>	<p>If the above address is incorrect please enter the organisation's correct address below</p>
--	---

2. Introduction

Civil Service Pensions, Department of Finance is committed to complying with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018. Department of Finance (DoF) Data Protection Policy requires Data Sharing Agreement(s) [DSA] to be put in place to help safeguard the use and handling of personal / special category data. This DSA covers the sharing of data between (hereafter called the other party) and Civil Service Pensions, Department of Finance (DoF) to fulfil various business requirements. A glossary of terms used in this DSA can be found at Annex 2.

This DSA does not give unrestricted access to information the other party may hold but sets out the parameters for the safe and secure sharing of personal/special category data for a justifiable need to know purpose.

The primary function of Civil Service Pensions is the administration of the Northern Ireland Civil Service Pension Schemes and their associated schemes which include the Civil Service Injury Benefits Scheme (Northern Ireland) 2003 [CBISB(NI)2003] and the Civil Service Compensation Scheme (Northern Ireland) [CSCS(NI)].

Personal / special category data includes information about living identifiable individuals that allows you to distinguish one person from another. Examples include: name, address, ID codes, bank details and health records (physical or mental). (This is not an exhaustive list).

3. Purpose

In order to fulfil the statutory obligation to provide members of the NICS pension schemes with accurate and timely benefits, personal data must be shared between Pensions Division and *[Employer]*.

The impact of not being able to share data will result in:

- scheme benefits not being paid or paid inaccurately;
- financial loss to the public purse;

- the non-issue of Annual Benefit Statements/Pension Saving Statements;
- complaints and reputational damage to Pensions Division/Department of Finance; and
- non-compliance with statutory obligations.

4. Legal Basis for Data Sharing

The sharing of data between Civil Service Pensions and the other party is necessary under Article 6(1)(c) of the GDPR in order to adhere to the Department of Finance's legal obligation to administer the NICS pension schemes. The NICS pension schemes are administered in accordance with and in compliance with the following legislation:

- Superannuation (Northern Ireland) Order 1972
- Public Services Pensions Act (Northern Ireland) 2014
- General Data Protection Regulation / Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003 (as inserted by the Serious Crime Act 2007)
- Human Rights Act 1998
- Digital Economy Act 2017

The processing of special category personal data is necessary for reasons of substantial public interest (Article 9(2)(g) of the GDPR), specifically in relation to Schedule 1, Part 2 Paragraph 21 of the Data Protection Act 2018 (Occupational Pensions).

All parties involved in this DSA will adhere to the six Data Protection Principles contained in the General Data Protection Regulation (GDPR). The six principles which are legally enforceable by the Information Commissioner state that personal data must be:

- i) processed lawfully, fairly and in a transparent manner;
- ii) collected for specified, explicit and legitimate purposes;
- iii) adequate, relevant and limited to what is necessary;
- iv) accurate and where necessary kept up to date;
- v) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which those data are processed;
- vi) processed in a manner that ensures appropriate security of the personal data.

5. Organisations involved

Data will be shared between Civil Service Pensions and the other party as outlined within this agreement to facilitate business need. Key members of staff involved are as follows:

Pensions Division

Name	Organisation	Position	Email address
Grace Nesbitt	Pensions Division (Department of Finance)	Information Assurance Officer (IAO) Pensions Division Director	Grace.nesbitt@finance-ni.gov.uk
Margaret Coyle	Civil Service Pensions (Department of Finance)	Deputy IAO / Head of Civil Service Pensions Policy, Legislation and Communications	Margaret.coyle@finance-ni.gov.uk
Anne Stewart	Civil Service Pensions (Department of Finance)	Deputy IAO / Head of Civil Service Pensions Operations	anne.stewart@finance-ni.gov.uk
Jenny Lynn	Department of Finance	Data Protection Officer	DataProtectionOfficer@finance-ni.gov.uk

Please complete contact details of key members of staff

Name	Position	Email address

Data will be shared as appropriate and relevant to each case. Civil Service Pensions may pass certain details to delivery partners or a third party responsible for carrying out an administrative function of the Scheme. A list of information Civil Service Pensions may share with third parties is provided at Annex 1. (This may not be an exhaustive list).

6. Data to be shared

Types of data to be shared between Civil Service Pensions and the other party including special category data are set out below:

- Name, titles and other forms of address;
- Date of Birth;
- Addresses (Home and Work);
- National Insurance number;
- Telephone numbers, if provided;
- Email address, if provided;
- Marital Status and effective dates of changes;
- Pension Scheme(s) to which member has belonged and effective dates;
- Employee Grade Code, including Industrial / Non-Industrial categorisation;
- Salary, Allowance and Bonus data and effective dates (start / end);

- Pensionable and Non-Pensionable categorisation of service in the pension schemes and effective dates (start / end);
- Scheme Contributions, including member, employer, Added Years, Added Pension, EPA;
- CARE Benefits details for nuvos and alpha members;
- Dates of joining, leaving / retiring from Scheme (including death);
- Non-reckonable service;
- Reason for Leaving (e.g. Resignation, Age Retirement, Ill Health Retirement, Partial Retirement, Actuarially Reduced Retirement, Transfer Out, Dismissal/Inefficiency, Death (in service, in retirement, in deferment));
- Dates of Opting in or Out of the pension schemes;
- Results of all calculations of entitlements under the scheme, whether for estimate, Annual Allowance, Annual Benefit Statement or payment of benefits purposes;
- Details of billing for lump sums, pensions;
- Medical certification of Ill-Health / Serious Ill-Health retirement;
- Medical certification of entitlement to benefits under the Civil Service Injury Benefit Scheme (Northern Ireland);
- Birth, Death, Civil Partnership, Divorce Certifications/Decrees;
- Temporary Injury Application Booklet / Permanent Injury Application Booklet,
- Overpayment information, if appropriate.

This is not an exhaustive list.

All data assets will be recorded in the DoF Information Asset Register.

Data to be shared will be specific / unique to each case and vary from case to case.

Data may be combined and/or linked with other data received to process benefits due and/or update members records.

7. Information use

Data sharing will take many forms, i.e. case by case; information on block, or ad hoc shares.

Both parties will undertake that the information shared under this DSA will only be used for the specific purpose for which it was shared, e.g. pension benefit purposes.

In each case, the originating party remains the primary owner and record keeper for the information that is shared. Therefore, in some instance, data may be passed back and forth between each party. Where the information is edited by the receiver, they must make it clear this is an altered copy and have sought agreement from the party prior to any alteration taking place.

The recipient will not release the information to any third party without obtaining the express written authority of the party who provided the information. The information shared with the third party will only be used for the specific purpose for which it was shared, i.e. pension benefit purposes. A list of third parties with whom information may be shared either as a legal requirement or at the request of the individual to whom the personal data relates can be found at Annex 1.

All shared information, personal or otherwise, must only be used for the purpose specified at the time of disclosure and set out in this agreement unless in compliance with the statutory provision or a court order. Data Protection legislation requires that any information shared is adequate, relevant and limited to what is necessary.

If a party decides not to disclose some or all of the personal data, the requesting authority must be informed. For example, a party may be relying on a lawful exemption from disclosure or on the inability to obtain consent from a data subject.

Under the Data Protection Act 2018 and GDPR, an individual is entitled, to request releasable copies of any records held about them.

If a party ceases to be part of this DSA, both parties must agree on what should happen to the information that has already been shared between them i.e.

- The information that has already been shared with the other signatory by the departing party/organisation.
- The information that has already been shared with the departing organisation/party by the other signatory.

An agreed method of returning or securely destroying the data will be drawn up as appropriate. (See Section 11 - Retention and Disposal).

8. Requests for information

In the event of a Data Subject Access Request, Freedom of Information request, Environmental Information Regulation or a Human Rights request, it will be co-ordinated and replied to by the Data Controller of the data. This must be replied to by the stipulated timeframe associated with the type of request. These replies should be in line with overarching policy, procedures and principles of the relevant Regulations/Acts and ensure that they are not contravened.

9. Responsibilities of each party

Under this DSA Civil Service Pensions and the other party will in the event of a breach of this agreement which results in a claim or proceedings, agree to co-operate to identify and apportion responsibility for the breach and the defaulting party will accept responsibility for any such claim. As such, both parties are responsible for complying with Data Protection Legislation and the agreement defines responsibilities in relation to the specified elements of processing. Each party is responsible for complying with this DSA to ensure lawful use for the safe, secure sharing and handling of personal / special category data for which they have responsibility. Each party is responsible for ensuring that they meet the conditions set out in Data Protection legislation when processing personal / special category information. In addition, they will ensure that the additional conditions required for the processing of information classed as special category personal data are met to ensure that the information is used and disclosed lawfully.

The DSA does not give unrestricted access to information that the other party may hold but sets out the parameters for the justified need to know purpose.

Each party will ensure that the information provided is both accurate and up to date

Each party will ensure that staff are only given access to personal data where there is a legal right, in order for them to perform their duties in connection with the delivery of that service.

Each party is responsible for ensuring that any staff accessing information under this agreement have been trained in Data Protection and are fully aware of their responsibilities to maintain the security and confidentiality of any personal information.

Each party should ensure that any staff accessing information under this DSA follow the procedures and standards that have been agreed and incorporated within this DSA and have received appropriate GDPR / Data Protection training.

Each party must have a Retention and Disposal Policy or similar policy in place.

The party originally supplying the information should be notified immediately of any breach of confidentiality or incident involving a risk to or breach of the security of information.

Neither party should assume that any non-personal information is not sensitive and can be freely shared. The party from whom the information originated should be contacted before any further sharing takes place.

Each party is responsible for ensuring that they have organisational and security measures in place to protect the lawful use of information shared. Each will ensure a reasonable level of security for supplied information and process the information accordingly.

Each party will comply with the six data protection principles in all their processing of the data being shared. The ICO Data Sharing code of practice which is currently being updated will explain in detail how the Data Protection Act 2018 applies to the sharing of personal data.

Each party will have a **Privacy Notice** stating the purposes of their processing activities and reflecting the sharing arrangements agreed.

Each party reserve the right to carry out an audit or review of the other party's compliance within the terms of this DSA and both parties agree to co-operate fully with any such review or audit. The parties will give 28 days' notice of any such review.

Each party will share with the other party the outcome of any audits or reviews that have been carried out on its activities.

10. Security

Both parties will take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss to, destruction of, or damage to, personal data.

Civil Service Pensions will use the SFTP Service provided through Enterprise Shared Services/IT Assist to transfer data securely to and from delivery partners and third party suppliers. This is a network protocol that provides file access, file transfer and file management functionalities over any reliable data stream.

This Data is received by interface, email, SFTP (Secure File Transfer Protocol, courier, recorded delivery or personally from the member.

IT systems in use within Civil Service Pensions are password protected.

The use of HPRM within Civil Service Pensions with access restrictions is in place.

Data will be marked with the appropriate Government Security Classification.

As applicable, acknowledgments of receipt of data will be supplied by the other party.

Data stored on drives are subject to strict access controls.

Both parties should ensure that staff are trained to ensure the physical and IT security of the data in line with Data Protection procedures are adhered to. This will include guidance for the issuing of information by email, fax, mail and courier. As applicable staff are trained regarding these measures when they are working away from the office and also when using encrypted laptop or mobile devices. Written Data Protection Procedures will be regularly communicated to all staff.

Both parties will ensure that only people/staff who have a genuine business need to see the data will have access to it.

11. Retention and disposal

Within Civil Service Pensions data will be retained for whichever is the greater of either a period of 7 full calendar years following the previous fiscal year in which the file has been closed or whatever is stated in the Department of Finance Retention and Disposal Schedule. Other parties should have similar processes in place.

In each case, the originating party remains the primary information owner and record keeper for the information which is shared. Where information has been edited by the receiver, following express written authority from the originating party, the receiver must make it clear that it is an altered document.

The receiving party will not release the information to any third party not connected with the case without obtaining the express written authority of the partner who provided the information.

An agreed method of returning or securely destroying the data will be drawn up as appropriate. The Department of Finance Retention and Disposal Schedule governs all Civil Service Pensions records and determines the destruction process in line with legislation and in conjunction with the Public Record Office Northern Ireland (PRONI). Receiving parties should have a similar process in place.

12. Security Incidents or Data breaches

Within Civil Service Pensions, all security incidents or data breaches will be dealt with according to the [Department of Finance Data Breach Management Plan](#) and adhering to the set policy and guidelines. The other party should have similar policy and guidelines in place.

In the first instance the Information Asset Owner (IAO) / responsible nominated officer within the area of the branch/incident will initiate any required action.

In the event of a breach of this agreement which results in a claim or proceedings, the parties agree to co-operate to identify and apportion responsibility for the breach and the defaulting party will accept responsibility for any such claim and each party must fully engage in the resolution of an incident by assisting in the investigation being carried out by the responsible partner.

13. Review/ Termination of Data Sharing Agreement

This DSA will be reviewed triennially. If applicable and practical, the timing of such will correspond with the review date of any Participation Agreement in place.

The person responsible for initiating this process will be the IAO (or equivalent) in each party or any such deputy they appoint to carry out this task.

This DSA may be varied only by prior written agreement between the parties.

Either signatory to this DSA can request an extraordinary review at any time.

Should any significant change take place which means that this DSA becomes an unreliable reference point, the DSA will be updated as needed and a new version signed by both parties will be issued to both parties for retention.

Should either party wish to terminate this DSA, a full financial year's notice in writing must be sent to the other party unless exceptional circumstances apply, e.g. misconduct.

In the event of the termination of the DSA the receiver shall delete from its records all the shared information in line with the Department of Finance Retention and Disposal Policy or equivalent schedule. The receiver should ensure secure deletion or disposal of all shared data and as applicable record actions on its Retention and Disposal Schedule or equivalent schedule to reflect this and advise the other party accordingly.

14. Indemnity

In the event of a breach of this agreement which results in a financial penalty, claim or proceedings, the parties agree to co-operate to identify and apportion responsibility for the breach and the defaulting party will accept responsibility for any such claim.

This page is intentionally left blank

15. Signatures

I have read, understood and agree to abide by the terms and conditions of this Data Sharing Agreement. All information will only be used for the purpose defined and listed in this agreement.

Signed on behalf of Civil Service Pensions

Name (Block Capitals):

Position: _____

Date: _____

Signed on behalf of the

(This should be the Senior Responsible Officer or equivalent within the organisation)

Name: (Block Capitals):

Position: _____

Date: _____

This page is intentionally left blank

INFORMATION PENSIONS MAY SHARE WITH THIRD PARTIES. Please note that this is not an exhaustive list.

Third Party	Information	Controls in place to protect information.
NI Audit Office, Internal Audit, Public Prosecution Service and other public sector bodies where relevant.	Personal Data as appropriate to each case	Data sharing agreement in place. Where possible data transferred by HPRM, GSI, GSE, SFTP, or secure interface. Where possible documents will be placed into HPRM, and the access will be restricted. External courier and postal services.
Departmental Solicitors Office	Personal Data as appropriate to each case	Data sharing agreement in place. Where possible data transferred by HPRM, GSI, GSE or SFTP. Where possible documents will be placed into HPRM, and the access will be restricted. External courier and postal services.
Pensions Ombudsman (PO) and The Pensions Advisory Service (TPAS)	Personal Data as appropriate to each case at the request of the PO and TPAS with the authority of the member.	Where possible data transferred by SFTP, GSI, GSE or secure email. External courier and postal services.
Benenden, Civil Service Health Care Society, Civil Service Pensioners Alliance, Civil Service Retirement Fund, Civil Service Sports Association, Give As You Earn, NICS Sports and Social Club, NI Prison	Personal Data – each organisation supplied with selection of Civil Service Pension Number, Name, NINO and amount to be deducted/paid at the request of the member.	Data emailed via password protected excel spreadsheet

Benevolent Fund, Norwich Union, UK Civil Service Benevolent Society Charity for Civil Servants.	Civil Service Pensioners Alliance also receives address if requested by member.	
Public Representatives	Personal data as applicable to the individual case with the authority of the member.	Response letters following representation made by members to MLAs, MPs etc. with member's authority. (The Private Office requires sight of all responses before issue).
External pension providers: Standard Life, TUC Prudential, Equitable Life, Scottish Widows	Name: DOB: Member number: NINO: Marital status: Leaving Reason:	Secure email and postal services.
HMRC	Personal and Payroll data	Submissions made through Capita Employee Services (CES), HMRC website or Electronic Data Interchange (EDI).
Government Actuary's Department	Personal Data as appropriate to each case	SFTP or Secure portal used
National Fraud Initiative (& participating bodies)	Personal and Payroll Data (Biennial exercise) Mortality Screening Exercise.	Data uploaded through NFI secure website and password protected files as their preferred method of receipt.
DoF Central Investigation Unit	To supply personal information to assist in the detection of fraud/crime.	Secure emails. Hard copies as requested.

HRCconnect/Fujitsu	All personal and pension data individual to the case	Via SFTP. HRCconnect are fully aware of their data protection responsibilities as set out in contract between CSP and HRCconnect.
PSNI	Personal information as requested for individual cases.	Pensions Division providing information as and when requested as PSNI have necessary legislation to support requests. PSNI responsible for destruction of same.
Account NI	Customer personal information and personal NICS/DoF staff information	Secure portal and internal email. Account NI as part of ESS Directorate adhere to DoF data protection policy.
DoF Finance Division	Staff, customer and supplier and personal information	Via secure email. HPRM

This page is intentionally left blank

GLOSSARY

Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003 – provides the statutory powers to the Comptroller and Auditor General (C&AG) to conduct data matching exercises for the purpose of assisting in the prevention and detection of fraud.

Data Controller – a person or organisation (either alone or jointly or in common with other persons or organisations) determines the purposes for which and the manner in which any personal information is to be processed.

Data Protection Act 2018 – updates data protection laws in the UK supplementing the EU Law Enforcement Directive and extending data protection laws to areas which are not covered by the GDPR.

Data protection principles – six rules which all organisations processing personal data must conform to.

Data Sharing Agreement (DSA) - an agreement setting out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

Data sharing – the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. It can take the form of systemic, routine data sharing where the same information is shared between the same organisations for an established purpose, or one off decisions to share data for any of a range of purposes.

Data subject – an individual who is the subject of the personal data.

Environmental Information Regulations 2004 (EIR) – legislation that provides rights of public access to environmental information held by public authorities.

Environmental Information Regulation (EIR) request – a request by a member of the public for access to environmental information held by a public authority. In most cases, the public authority must provide a response to the request within 20 working days of receipt.

Freedom of Information Act 2000 – (FOI) - legislation that provides public access to information held by public authorities.

FOI request – a request from a member of the public for access to information held by a public authority. The public authority must provide a response to the request within 20 working days of receipt.

General Data Protection Regulation (GDPR) – a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR came into effect across the EU on 25 May 2018.

Human Rights Act 1998 - an Act of Parliament of the United Kingdom which came into force on 2 October 2000. Its aim was to incorporate into UK law the rights contained in the European Convention on Human Rights.

ICO Data sharing code of practice – his code explains how the Data Protection legislation applies to the sharing of personal data

Information Asset Owner (IAO) - the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately.

National Fraud Initiative - The Comptroller and Auditor General (C&AG) has statutory powers to conduct data matching exercises for the purpose of assisting in the prevention and detection of fraud. The powers are contained in Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003 as inserted by the Serious Crime Act 2007.

Personal data – information which relates to a living individual who can be identified from that information and other information in the possession of the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notice – a public document from an organisation that explains how the organisation processes personal data and how it applies the data protection principles.

Processing of data – is any activity involving the information / data. This includes obtaining, recording or holding the data or doing any work to it such as organising, adapting, changing, erasing or destroying it.

Public Services Pensions Act (Northern Ireland) 2014 - This Act establishes reformed public service schemes in Northern Ireland which will operate from 1 April 2015. The powers in the Act broadly supersede powers to create schemes for the payment of pensions and other benefits under different legislation including the Superannuation (Northern Ireland) Order 1972.

SFTP – Secure File Transfer Protocol – More information regarding SFTP is available from IT Assist catalogue. http://itassist.nigov.net/our_services

Special category data – personal information about an individual's race or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; health; sexuality; criminal proceedings or convictions. Special category data can only be processed under strict conditions.

Subject access request/data subject access request (DSAR) – a written request from an individual for information is held about them. The data controller must respond to the request within 40 calendar days of receipt.

Superannuation (Northern Ireland) Order 1972 – This Order provides an authority for some of the pension and compensation schemes operated for Northern Ireland civil servants and eligible related employments.