SPORT NORTHERN IRELAND

Data Protection Policy Statement

Date of Implementation:	
Date of Review:	September 2022
Date of Next Review:	August 2025
Summary of Changes:	Complete Revision
Approved by Board:	October 2022

DOCUMENT REF:	Data Protection Policy Statement
AUTHOR:	Information Management Service
RESPONSIBLE OWNER:	Chief Operating Officer
LINKED DOCS:	Data Loss Handling Plan Data Management Policy Information Assurance Framework Information Security Policy Access to Information Policy Freedom of Information Policy and EIR Procedures Manual Data Sharing Guidelines Record Management Policy Record Management Handbook Senior Information Risk Officer Handbook Social Media Policy Retention and Disposal Policy Information Asset Register Information Asset Register Guidance Publication Scheme

DOCUMENT CONTROL

Version	Date	Changes
V2	**October 2022**	**Approved by COO/SIRO to go to Board for approval**
V1	**September 2022**	**Reviewed by Interim Information Support Officer**

CONTENTS

1. Introduction and Scope

Sport Northern Ireland is fully committed to complying with UK data protection legislation. Sport Northern Ireland will follow procedures to ensure that all employees, contractors, consultants, and other parties who have access to any personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under these laws.

2. Legislative Context

Historically, Data Protection has been governed by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 giving effect in UK law to EU Directive 95/46/EC. Together they formed the framework for regulating the methodologies for the collection and processing of personal data in the UK from 25 May 2018, replacing the former Data Protection Act 1998.

The General Data Protection Regulation (GDPR) ceased having a direct effect in the UK on 01 January 2021 (Brexit 'Exit Day') in protecting the rights and freedoms of UK Citizens regarding their personal information. The UK, however, did commit to the maintenance of an equivalent data protections regime and the UK version of GDPR, UK General Data Protection Regulation, applied from 1 January 2021. The UK Government also published an update to the Data Protection Act 2018 called the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ('EU Exit Regulations'). This UK GDPR was established by the European Union (Withdrawal) Act 2018, which incorporates the body of EU law (including the GDPR) as it existed on the day the UK exited from the EU and was incorporated into UK law known thereafter as (UK GDPR). It carries much of the existing principles of EU GDPR legislation but is only relevant within the UK. It sets out the key principles, rights, and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

The Data Protection Act 2018 remains in place but is effectively now subordinate to the UK GDPR. The UK General Data Protection Regulation, it is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ('EU Exit Regulations') applies a number of necessary changes to the GDPR to make it relevant to the UK following departure from the EU. For example, it removes

references to cross-border data transfers with other Member States and participation in EU wide-institutions such as the European Data Protection Board (EDPB).

3. Statement of Policy

Sport Northern Ireland needs to collect and use information about people with whom the organisation works, to conduct business and provide services. These may include members of the public, current, past, and prospective employees, clients, customers and suppliers. In addition, Sport Northern Ireland may be required by law to collect and use information. All personal information, whether in paper, electronic or any other format, must be handled and managed in accordance with the UK General Data Protection Regulation and EU GDPR legislation. This policy statement should be read in conjunction with all linked documents outlined above, however, particular attention should be paid to the following policies: the Data Loss Handling Plan, Freedom of Information Policy and the Access to Information Policy.

4. Management and Responsibilities

Sport Northern Ireland is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data processed by us about customers, staff or those who work or interact with us.

See Annex A for organisational chart for SIRO /IAO structure and responsibility

Information Asset Owners – Sport Northern Ireland assigns an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities support Sport Northern Ireland in managing personal data and its associated risks.

Privacy Notices - Sport Northern Ireland publishes a privacy notice on the website and provides timely notices where this is required. Sport Northern Ireland tracks and makes available any changes in the privacy notice. Sport Northern Ireland also publishes a staff privacy notice and keep it up to date. Sport Northern Ireland publishes a privacy notice on the organisation's website and publications. It can be viewed here: Sport Northern Ireland Freedom of Information and Privacy Notice.

5. Definition

The UK General Data Protection Regulation definition of "personal data" includes any information relating to an identified or identifiable natural living person. Pseudonymised

personal data is covered by this legislation, however anonymised data is not regulated by the UK GDPR or the Data Protection Act 2018, providing the anonymisation has not been done in a reversible way.

Some personal data is more sensitive and is afforded extra protection, this is information related to:

• Race or ethnic origin;

• Political opinions;

• Religious or philosophical beliefs;

• Trade union membership;

• Genetic data;

• Biometric ID data;

• Health data;

• Sexual life and/or sexual orientation; and

• Criminal data (convictions and offences).

This policy should be read in conjunction with the following Sport Northern Ireland policies and procedures:

i. Data Loss Handling Plan;
ii. Data Management Plan;
iii. Information Assurance Framework;
iv. Information Security Policy;
v. Access to Information Policy;
vi. Freedom of Information Policy and EIR Procedures Manual;
vii. Data Sharing Guidelines
viii. Records Management Policy;
ix. Records Management Handbook;
x. Senior Information Risk Officer Handbook;
xi. Social Media Policy;
xii. Retention and Disposal Policy;
xiii. Information Asset Register;
xiv. Publication Scheme; and
xv. Freedom of Information / Privacy Notice.

6. Data Protection Principles

Sport Northern Ireland fully supports and complies with the principles of UK and EU Data Protection legislation. UK GDPR sets out seven key data protection principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Sport Northern Ireland endeavours to ensure that these principles lie at the heart of the organisation's approach to processing personal data.

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

- "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) 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 with delay ('accuracy');
- (e) 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 period 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 ('storage limitation'); and

- (f) 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')."

Article 5(2) adds that:

- "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

EU GDPR also recognised the rights to privacy and data protection as fundamental rights set out in Article 7 and 8 of the EU Charter of Fundamental Rights. There is a specific legislative act for institutions, bodies, offices and agencies of the European Union Regulation (EU) 2018/1725 that also applies to the European External Access Service (EEAS) when processing personal data. The renewed legal framework intends to guarantee an elevated level of data protection when it comes to collecting and storing personal data for the benefit of Union citizens and of external partners all over the world. It is harmonised with the principles of the EU GDPR.

In practice, this means Sport Northern Ireland must have appropriate security to prevent any personal data Sport Northern Ireland holds being accidentally or deliberately compromised.

7. Understanding and assessing risk in personal data breaches

It is up to staff in Sport Northern Ireland to risk assess any data breach. For further support and information, see the Sport Northern Ireland 'Data Loss Handling Plan' and associated documents, which provide an overview of procedures and processes to be followed in relation to the loss of data. The Information Owner needs to retain a record to explain how Sport Northern Ireland has assessed the breach, the risk and the decision on the outcomes. This is to ensure that Sport Northern Ireland has a record of all incidents and the outcome of investigations into any data breach, should there be a complaint to the Information Commissioner's Office (ICO) with a concern that personal information has been shared. The Information Owner needs to justify that an investigation was conducted, decisions were reached, procedures were followed and that an internal record was made.

It is important that all data breaches are dealt with promptly and in line with Sport Northern

Ireland policies as well as the timescales set out by the Information Commissioner's Office. Further information is available here 72 hours - ICO information on how to respond to a personal data breach

Remember, it is important that Sport Northern Ireland staff immediately conduct a risk assessment to demonstrate the organisation's awareness. Human error does occur; however, Sport Northern Ireland must prove that Sport Northern Ireland staff have taken all steps to reduce the likelihood of a similar breach reoccurring.

Sport Northern Ireland staff are all provided with GDPR training.

8. Registration with the Information Commissioner's Office

Sport Northern Ireland's purpose for holding personal information and a general description of the categories of people and organisations to which Sport Northern Ireland may disclose it to are listed in the Information Commissioner's Office (ICO) Data Protection Register (Registration number: Z8579526).

9. Data Processors

Where Sport Northern Ireland uses a contractor to process personal data on its behalf, the contractor must sign a data processing agreement, which ensure that they are taking adequate steps to comply with the Data Protection legislation and act only on the instruction of Sport Northern Ireland as agreed. Sport Northern Ireland and the data processors are responsible for their actions in processing personal data.

10. Individual's Rights

Under the Data Protection legislation, individuals have the following rights:

i. the right to be informed;
ii. the right to access;
iii. the right to rectification;
iv. the right to erasure;
v. the right to restrict processing;
vi. the right to data portability;
vii. the right to object; and
viii. rights in relation to automated decision making and profiling.

All requests to facilitate the exercise of data subject rights under Articles 15-22 of the UK GDPR will be facilitated.

11. Disclosure of Personal Information

Strict conditions apply to the passing of personal information both internally and externally. Sport Northern Ireland will not disclose personal information to any third party unless Sport Northern Ireland believes it is lawful to do so. Respect to confidentiality will be given, where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available, provided that:

- Sport Northern Ireland has the statutory power or is required by law to do so;
- The information is clearly not intrusive in nature;
- The member of staff has consented to the disclosure; or
- The information is in a form that does not identify individual employees.

12. Handling of Personal Information

All Sport Northern Ireland staff will, through appropriate training and responsible management:

- Fully observe conditions regarding the fair collection and use of personal and sensitive personal information;
- Meet Sport Northern Ireland's legal obligations to specify the purposes for which personal information is collected and processed;
- Collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality and accuracy of personal information used;
- Apply strict checks and appropriate data retention schedules to determine the length of time personal information is held;
- Ensure that the rights of people about whom information is held can be fully exercised under the UK GDPR;
- Respond to subject access requests promptly and within a 40-calendar day deadline;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without adequate safeguards; and
- Ensure all personal data is held in line with organisational records management policy.

13. Compliance

To assist in achieving compliance, Sport Northern Ireland has:

- Appointed a Senior Information Risk Owner (SIRO) who takes overall ownership of the organisation's information risk policy and is responsible for ensuring that information within the organisation is managed appropriately;
- Appointed Information Asset Owners (IAOs) who are responsible for the secure management of information within their business areas. They ensure that any data being disclosed remains secure and will investigate any data security incidents;
- Appointed an Information Manager (IM) to provide policy and guidance on data protection within the organisation; and
- Created a Records Management handbook, providing detailed guidance on data protection procedures.

Sport Northern Ireland will ensure that:

- There is always someone with specific responsibility for data protection in the organisation;
- Senior Information Responsible Owners (SIROs) and Information Asset Officers (IAOs) are assigned appropriate responsibilities to cover all business areas of Sport Northern Ireland. Regular training is provided for SIROs and IAOs. Registers are updated as required and schedules for updating registers are in place.
- Every two years SIROs and IAOs are reminded of their obligations under UK General Data Protection Regulation (UK GDPR);
- Everyone managing and handling personal information understands that they are directly and personally responsible for following good data protection and records management practice;
- Only staff who need access to personal information as part of their duties are authorised to do so;
- All staff have a specific data protection objective included in annual personal performance agreements;

  Everyone managing and handling personal information is appropriately trained to do so;

  Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information knows who to speak to and where to seek advice;
- Queries about handling personal information are promptly and courteously dealt with;

- A regular review and audit is made of the way personal information is collected, held and processed;
- A regular review and audit is made of the way personal information is collected, held and processed;
- Procedures for handling personal information are clearly understood and available;
- Procedures for handling personal information are regularly assessed and evaluated; and
- Performance on handling personal information is regularly assessed.

14. Staff Responsibilities

While Sport Northern Ireland has overall responsibility for compliance with the implementation of data protection and relevant GDPR legislation. This policy is delegated to the Information Management Team with the Information Manager holding senior responsibility, the Senior Information Risk Owner and the Information Asset Owners. The Director of Legal, Governance and Research Services is designated as the Senior Information Risk Owner ('SIRO') for the organisation for the purposes of the Data Breach Management Plan. The Chief Operations Officer is responsible for ensuring this policy is communicated to all staff. Information Asset Owners ('IAO') are responsible for ensuring this policy is further communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal data in use within their business area. Advice or assistance regarding this policy or the GDPR is available from the Data Protection and Information Standards Officer.

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

- All staff will be appropriately trained in the handling of personal information and Sport Northern Ireland provide a Senior Information Risk Owner handbook for the SIRO;
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically; and
- individual passwords are not easily compromised.

15. Data Breaches

In the event of a data breach, staff should follow procedures set out in the Sport Northern Ireland Loss Handling Plan. The purpose of the plan is to ensure that a consistent and effective approach is applied to handling breaches. The plan sets out the arrangements for the management of incidents and details the roles of Sport Northern Ireland staff in reporting and investigating breaches.

16. Data Sharing

Data sharing means the disclosure of data form Sport Northern Ireland to a third party organisation or organisations. Before disclosing personal information to another organisation, staff will ensure that all sharing is lawful, fair, transparent and in line with the rights and expectations of data subjects.

A data sharing agreement defines a common set of rules to be adopted by organisations involved in a data sharing operation. Within Sport Northern Ireland, it is mandatory to have in place a data sharing agreement in all cases where personal information is shared. It is also considered good practice to have a data sharing agreement in cases where the organisation intends to share sensitive, non-personal information.

The EU GDPR adequacy decision implies that data can continue to flow from the EEA in the majority of cases because the EU has adopted adequacy decisions about the UK. However, this decision does not include data transferred for the purposes of immigration control or where UK immigration exemption is applicable. For further information see Data Protection Act (2018) Chapter 5 and ICO information on UK-based business or organisation subject to the UK GDPR and you transfer personal data to or from other countries (including European countries).

17. Complaints

The Act sets out rules about the way organisations can collect and use information about data subjects and Sport Northern Ireland is committed to processing their personal data in

accordance with those rules. However, if a data subject feels that Sport Northern Ireland has not handled their personal data in accordance with the Act, they can make a complaint to the Information Manager.

They can also complain to us if they are dissatisfied with the response from Sport Northern Ireland in relation to their subject access request for their own personal data. Normally, they will receive a reply within 20 working days after the date their complaint is received.

Data subjects are also entitled, under section 42 of the Act, to ask the ICO to make an assessment of whether or not the organisation is complying with the Act's provisions.

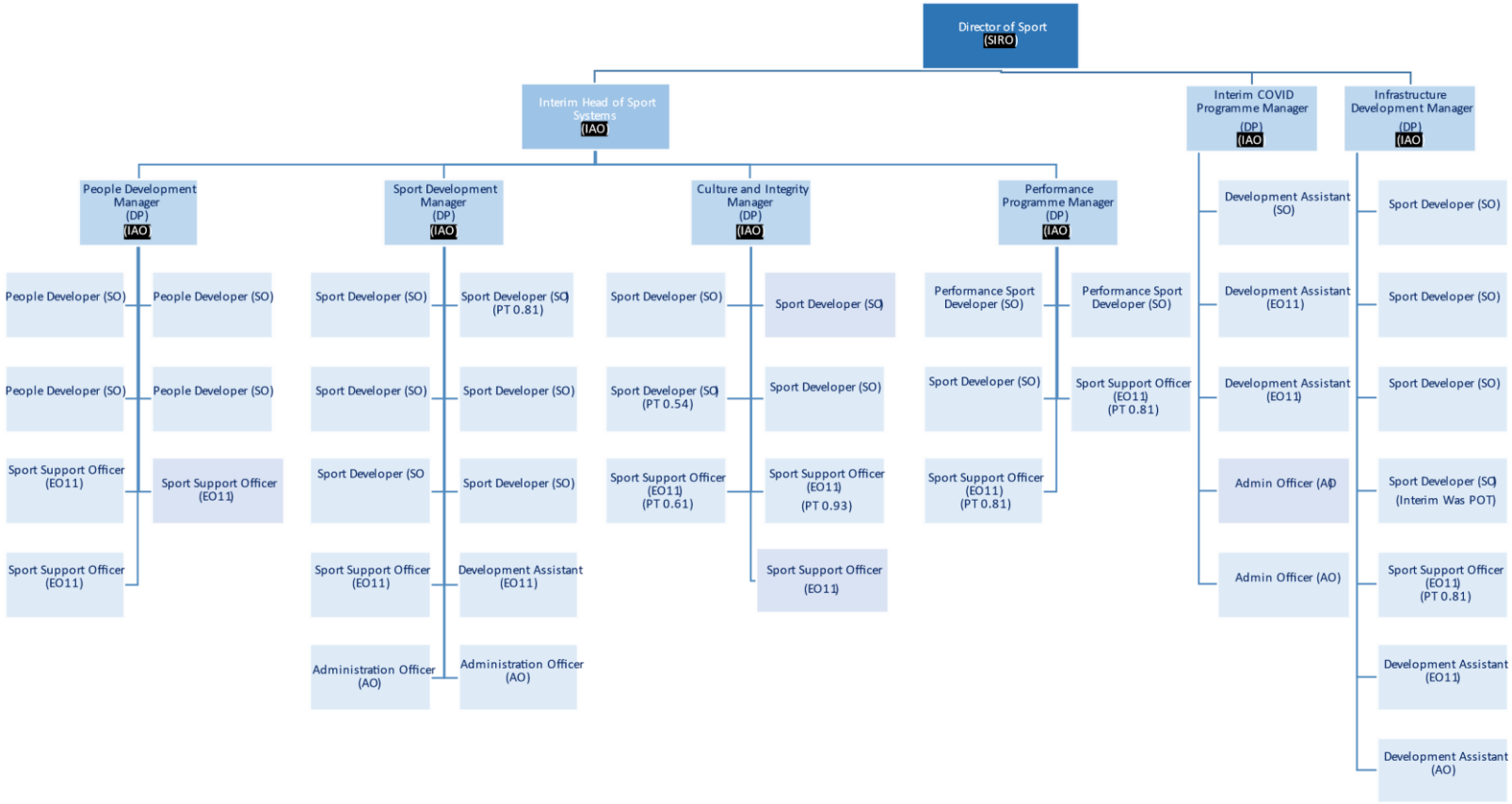
18. Third Party Users of Sport Northern Ireland Personal Information

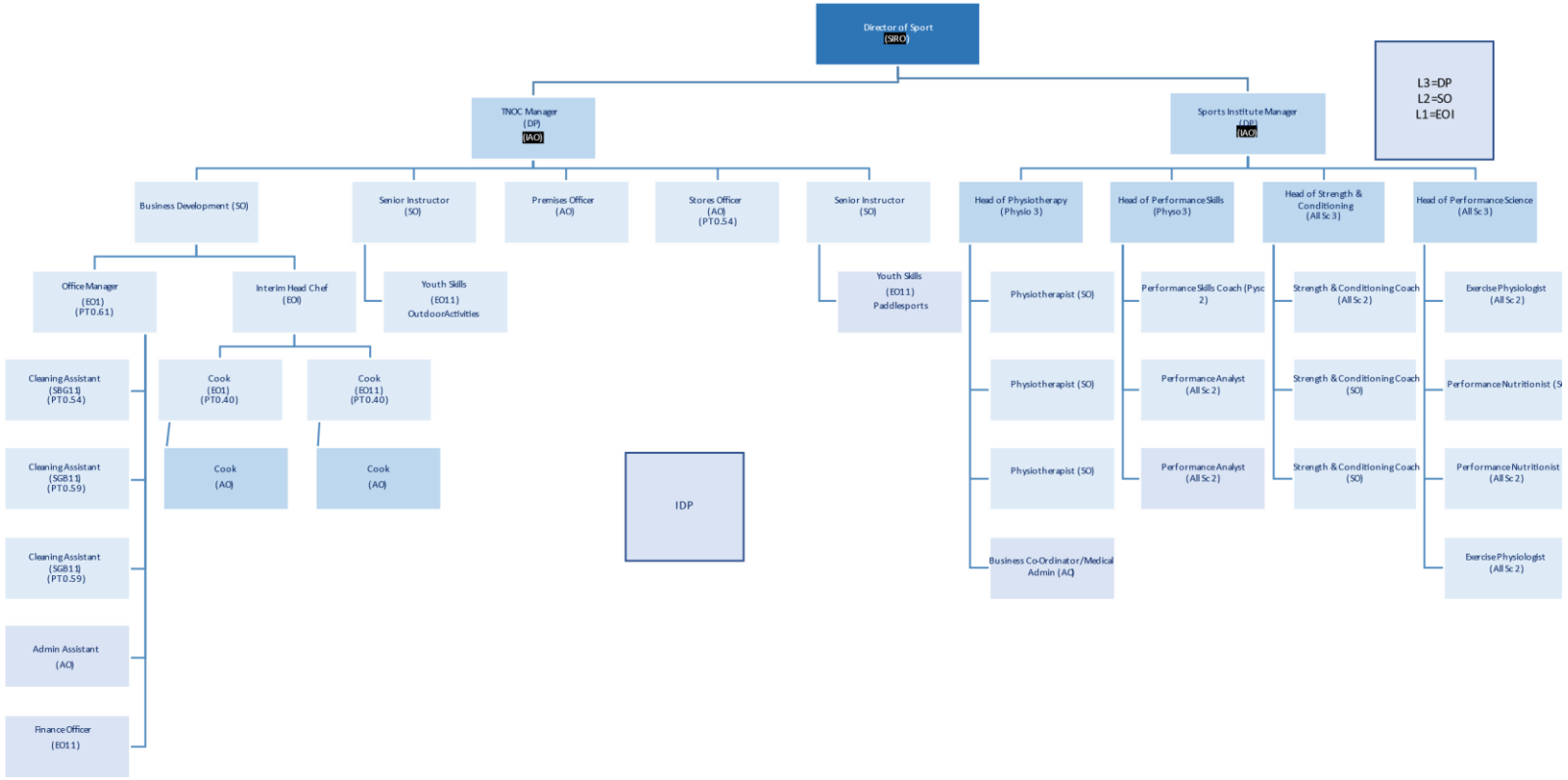
Any third parties who are users of personal information supplied by Sport Northern Ireland will be required to confirm and demonstrate that they will abide by the requirements of the Act. Audits will be conducted by the organisation to ensure compliance.

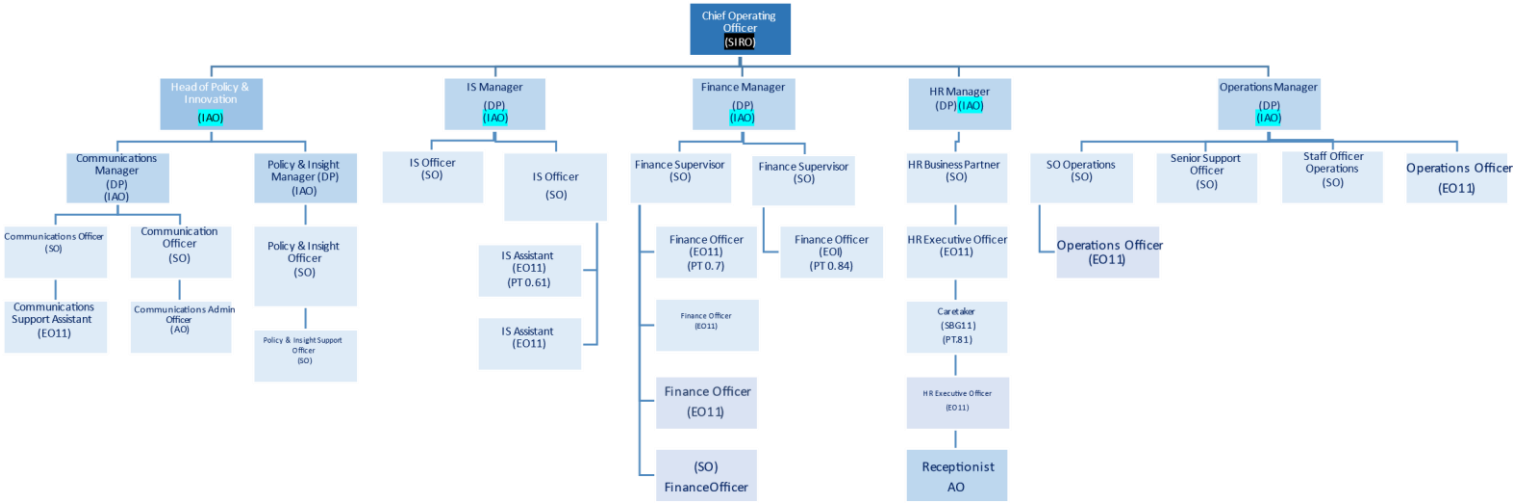
19. Policy Awareness

A copy of this policy statement will be given to all new members of staff and interested third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on Sport Northern Ireland's internet and intranet sites, as will any subsequent revisions. All staff and relevant third parties must be familiar with and comply with this policy at all times. This policy will be reviewed every 3 years, as a maximum.

Annex A Organisational Structure Chart for SIRO /IAO Chart staff responsibilities


Director of Sport
(SIRO)
Interim Head of Sport Systems
(IAO)
Interim COVID Programme Manager
(DP)
(IAO)
Infrastructure Development Manager
(DP)
(IAO)
People Development Manager
(DP)
(IAO)
Sport Development Manager
(DP)
(IAO)
Culture and Integrity Manager
(DP)
(IAO)
Performance Programme Manager
(DP)
(IAO)
People Developer (SO)
People Developer (SO)
People Developer (SO)
People Developer (SO)
Sport Support Officer (EO11)
Sport Support Officer (EO11)
Sport Support Officer (EO11)
Sport Developer (SO)
Sport Developer (SO) (PT 0.81)
Sport Developer (SO)
Sport Developer (SO)
Sport Developer (SO
Sport Developer (SO)
Sport Support Officer (EO11)
Development Assistant (EO11)
Administration Officer (AO)
Administration Officer (AO)
Sport Developer (SO)
Sport Developer (SO) (PT 0.54)
Sport Support Officer (EO11) (PT 0.61)
Sport Developer (SO)
Sport Developer (SO)
Sport Support Officer (EO11) (PT 0.93)
Sport Support Officer (EO11)
Performance Sport Developer (SO)
Sport Developer (SO)
Sport Support Officer (EO11) (PT 0.81)
Performance Sport Developer (SO)
Sport Support Officer (EO11) (PT 0.81)
Development Assistant (SO)
Development Assistant (EO11)
Development Assistant (EO11)
Admin Officer (AO)
Admin Officer (AO)
Sport Developer (SO)
Sport Developer (SO)
Sport Developer (SO)
Sport Developer (SO) (Interim Was POT)
Sport Support Officer (EO11) (PT 0.81)
Development Assistant (EO11)
Development Assistant (AO)


Director of Sport
(SIRO)
TNOC Manager
(DP)
(IAO)
Sports Institute Manager
(DP)
(IAO)
L3=DP
L2=SO
L1=EOI
Business Development (SO)
Senior Instructor
(SO)
Premises Officer
(AO)
Stores Officer
(AO)
(PT0.54)
Senior Instructor
(SO)
Head of Physiotherapy
(Physio 3)
Head of Performance Skills
(Physo 3)
Head of Strength &
Conditioning
(All Sc 3)
Head of Performance Science
(All Sc 3)
Office Manager
(EO1)
(PT0.61)
Interim Head Chef
(EO)
Youth Skills
(EO11)
OutdoorActivities
Youth Skills
(EO11)
Paddlesports
Physiotherapist (SO)
Physiotherapist (SO)
Physiotherapist (SO)
Business Co-Ordinator/Medical
Admin (AO)
Performance Skills Coach (Pysc
2)
Performance Analyst
(All Sc 2)
Performance Analyst
(All Sc 2)
Strength & Conditioning Coach
(All Sc 2)
Strength & Conditioning Coach
(SO)
Strength & Conditioning Coach
(SO)
Exercise Physiologist
(All Sc 2)
Performance Nutritionist (S
Performance Nutritionist
(All Sc 2)
Exercise Physiologist
(All Sc 2)
Cleaning Assistant
(SBG11)
(PT0.54)
Cook
(EO1)
(PT0.40)
Cook
(EO11)
(PT0.40)
Cleaning Assistant
(SGB11)
(PT0.59)
Cook
(AO)
Cook
(AO)
Cleaning Assistant
(SGB11)
(PT0.59)
IDP
Admin Assistant
(AO)
Finance Officer
(EO11)


Chief Operating Officer (SIRO)
Head of Policy & Innovation (IAO)
IS Manager (DP) (IAO)
Finance Manager (DP) (IAO)
HR Manager (DP) (IAO)
Operations Manager (DP) (IAO)
Communications Manager (DP) (IAO)
Policy & Insight Manager (DP) (IAO)
IS Officer (SO)
IS Officer (SO)
Finance Supervisor (SO)
Finance Supervisor (SO)
HR Business Partner (SO)
SO Operations (SO)
Senior Support Officer (SO)
Staff Officer Operations (SO)
Operations Officer (EO11)
Communications Officer (SO)
Communication Officer (SO)
Policy & Insight Officer (SO)
IS Assistant (EO11) (PT 0.61)
IS Assistant (EO11)
Finance Officer (EO11) (PT 0.7)
Finance Officer (EOI) (PT 0.84)
HR Executive Officer (EO11)
Operations Officer (EO11)
Communications Support Assistant (EO11)
Communications Admin Officer (AO)
Policy & Insight Support Officer (SO)
Finance Officer (EO11)
Finance Officer (EO11)
Caretaker (SBG11) (PT.81)
(SO) FinanceOfficer
HR Executive Officer (EO11)
Receptionist AO