Northern Ireland
Fire & Rescue Service

NIFRS DATA PROTECTION POLICY & PROCEDURE

25 May 2018

Protecting Our Community

VERSION CONTROL	
Version Number:	5
Original Issue Date:	February 2006
Reviewed and Revised:	May 2009 July 2013 January 2015 May 2018
S75 Screening Date:	

Relevant Legislation

- The Data Protection Act 2018
- The Freedom of Information Act 2000;
- The Environmental Information Regulations 2004; and
- The General Data Protection Regulation (GDPR) 2018.

Linked Policies & Guidance Documents

This Data Protection Policy should be read in conjunction with, but not limited to, the following NIFRS documents:

- FOI Policy;
- Personal File Guidance;
- IS/IT Policy;
- Data Sharing Protocol;
- Information Governance Framework;
- Information Governance Strategy & Policy;
- Data Quality Policy;
- Publication Scheme;
- Code of Conduct and Code of Accountability for NIFRS Board Members;
- Staff Code of Conduct;
- Disciplinary Policy & Procedure;
- Good Management Good Records (GMGR);
- Brigade Circular 37/2006;
- Digital Imaging Policy;
- Social Media Policy;
- Media Handbook Policy; and
- Practical Guide to GDPR.

The above policies/guidance documents can be accessed via NIFRS Global Drive/Document Management System. The Publication Scheme is available in the Freedom of Information section of www.nifrs.org.

In addition to the above internal policies/guidance documents, external guidance can be accessed through the Information Commissioner's website www.ico.org.uk/.

1 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) which comes into force on 25 May 2018 define UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual who can be identified from the information.

NIFRS is committed to protecting the privacy of individuals and will ensure that it handles all personal information in a manner that complies with the GDPR. It is important to remember that data protection requirements have been in place for many years. Although GDPR does broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the current Data Protection Act.

It is the personal responsibility of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this Policy.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example, the Computer Misuse Act 1990 and the GDPR. All breaches will be investigated and appropriate action taken.

1.2 This NIFRS Data Protection Policy sets out how this personal data must be collected, handled and stored to meet data protection standards and to comply with the law.

2 POLICY STATEMENT

2.1 This NIFRS Data Protection Policy ensures that we:

- Comply with data protection law and follow good practice;
- Protect the rights of all stakeholders - staff, volunteers and other people we have a relationship with or may need to contact;
- Are open about how we store and process individuals' data; and
- Protect ourselves from the risks of a data breach.

2.2 The inappropriate use of information could have a significant effect on the efficient operation of NIFRS. This may result in restriction or loss of services to the public; financial or civil liability; or, ultimately, prosecution.

2.3 Information is collected because there is a need to share it, to record it for future use or to meet legal obligations. Access to timely, relevant and accurate information is, therefore, essential to support decision-making.

2.4 NIFRS is fully committed to protecting the privacy of all individuals, including staff, by ensuring the lawful use of any personal information held, in accordance with the GDPR.

3 AIMS OF THE POLICY

3.1 The NIFRS Data Protection Policy, supported by the NIFRS Practical Guide to GDPR and Information Governance policies, will ensure that:

- information and information systems are managed, maintained and used in a way that complies with GDPR whilst continuing to deliver information which is relevant, timely and accurate;
- all employees know, understand and implement the provisions of GDPR; and
- all employees abide by both their contractual and common law duty of confidentiality with regards to the data they handle in the course of their business.

4 GDPR PRINCIPLES

4.1 The General Data Protection Regulation (EU 2016/679) (GDPR) regulates how organisations collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be

collected and used fairly, stored and disposed of safely and not disclosed unlawfully.

4.2 The GDPR is underpinned by 6 important principles to which we will adhere (see Appendix A).

4.3 These 6 principles form the backbone of the GDPR and explain how personal information must be handled.

4.4 NIFRS, its staff and any others who process or use personal information on its behalf, must ensure that they follow these principles at all times.

4.5 As a direct result of these overarching principles NIFRS has developed the following best practice guidelines which cover in detail how we will achieve the above principles.

(a) All use and transfer of personal information within NIFRS will be clearly identified, supported by written procedures which have been fully justified at the appropriate level and regularly reviewed.
(b) We will only include personal data in information transfers where there is a clear business need to do so.
(c) When we do transfer data we will only transfer the minimum amount of data to meet the business need and we will regularly review what the minimum is.
(d) We will restrict access to personal data on a need to know basis based upon clearly defined business needs.
(e) All transfers out of the organisation will only occur once we are certain that the transfer is safe and secure and that we have a legal right to do so.
(f) Managers at all levels across the organisation will ensure that they and their staff are aware of these best practice guidelines and adhere to them.

5 COLLECTING PERSONAL INFORMATION

5.1 When personal information is collected, for example, on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice (see section 9).

5.2 Personal information collected must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

5.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see section 7 below). It must be made clear to the 'data subject' all the purposes that their information may be used for at the time the information is collected.

6 REGISTRATION & NOTIFICATION

6.1 The Information Commissioner's Data Protection Register contains a general description of the categories of people and organisations to which NIFRS may disclose personal information. The register is updated by the Information & Security Manager and can be searched at **http:/www.dpr.gov.uk.**

7 LAWFUL BASIS FOR PROCESSING

7.1 NIFRS has the right to process your personal data where there is a lawful basis to do so. In the majority of cases, our lawful basis will be at least one of the following applies:

- **Legal Obligation**: Processing is necessary for carrying out legitimate public duties of a Fire and Rescue Service as defined in the Fire & Services (Northern Ireland) Order 2006 and the Fire Safety Regulations (Northern Ireland) 2010.
- **Public Task**: Processing is necessary for us to perform a task in the public interest to help us in carrying out our public duty of improving, protecting and saving lives.

- **Vital Interests**: Processing is necessary to protect someone's life.
- **Contract**: For recruitment, employment, social security purposes or collective agreement.

There may be other occasions where we are required to process your personal data, however we will only do so where a lawful basis exists.

7.2 When NIFRS processes personal information, it must have a lawful basis for doing so. GDPR provides a list of 'conditions' when we can process personal or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations (see Appendix B).

7.3 The GDPR defines special category personal information as information relating to:

- race and ethnic origin;
- political opinion;
- religious or philosophical beliefs;
- trade union membership;
- processing of genetic/biometric data to uniquely identifying a person;
- physical or mental health or medical condition; or
- sexual life.

7.4 Whenever the Service processes personal information, it must be able to satisfy at least one of the conditions in Article 6 of the GDPR and when it processes 'special category' personal information, it must be able to satisfy at least one of the conditions in Article 9 of the GDPR as well.

7.5 The Service can process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes Special Categories of Personal Data – sensitive personal information see Appendix B). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded.

8 DATA PROTECTION ROLES & RESPONSIBILITIES

8.1 Whilst all staff and Board Members have a Data Protection responsibility, others have specific additional responsibilities and reporting lines as outlined below and shown diagrammatically at Appendix F.

8.2 NIFRS Board

Has ultimate responsibility for ensuring NIFRS complies with the requirements of the Legislation and discharge this responsibility through the Audit, Risk & Governance Committee.

8.3 Audit, Risk & Governance Committee

Receives quarterly reports on Data Protection and will report to the Board on issues arising.

8.4 Senior Information Risk Owner (SIRO)

The SIRO has overall corporate responsibility for Data Protection including keeping the Board updated about Data Protection responsibilities, risks and issues arising. The SIRO will ensure that NIFRS and its staff adhere to their Data Protection responsibilities and will actively monitor this through the procedures detailed in the NIFRS Information Management Assurance Framework.

They will lead the Information Management Group (IG), provide strategic direction to all IG leads.

The Director of Operations is currently NIFRS designated Senior Information Risk Owner (SIRO).8.5

8.5 Personal Data Guardian (PDG)

The Personal Data Guardian is responsible for monitoring the purpose and manner in which personal data is collected, processed, stored, shared and dispensed with and will work closely with the SIRO and Data Protection Officer to ensure compliance with GDPR.

The PDG is responsible in the first instance for the monitoring and sharing of data both internal and external to the organisation. All data access agreements will normally be vetted and approved by the PDG or in their absence by the SIRO.

Additionally the PDG is responsible for ensuring that the principles of privacy by design are incorporated into all new systems and process that will handle personal data. In these instances the PDG acts in the best interests of the Data Subject(s) not the organisation.

The Directors of Community Protection and Human Resources are NIFRS designated Personal Data Guardians.

8.6 **Information Security Manager**

The Information & Security Manager is responsible for the daily application of the Assurance Framework across NIFRS. On a day-to-day basis the Information& Security Manager will be responsible for the following tasks:

- Informing and advising employees of their data protection obligations;
- Monitoring compliance of policies and procedures. This includes monitoring responsibilities and training of staff involved in data processing;
- Reporting data breaches to the DPO and Information Commissioner;
- Ensuring the RoPA is an active register that identifies all systems that hold personal data;

- Advising on the necessity of Data Protection Impact Assessments (DPIAs), the manner of their implementation and outcomes;

- Serve as the contact point for all data protection issues, including managing risks and data breach reporting; and

- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

8.7 **Directors and Heads of Departments**

Day-to-day responsibility for Data Protection compliance is delegated by the Board through the Accounting Officer to the SIRO and to respective Directors/Heads of Departments for their service area.

8.8 **Data Protection Officer**

GDPR introduces a requirement to appoint or designate a Data Protection Officer (DPO) with formal responsibility for data protection compliance across NIFRS. This role is carried out by the Business Support Services (BSO) who will provide oversight and challenge roles as provided by the legislation.

8.9 **Head of Information Technology**

The Head of Information Technology is responsible for ensuring that all systems, services and equipment used for storing data meet acceptable security standards; regular checks are carried out to ensure security hardware and software is functioning properly; and evaluating any third party services that NIFRS is considering using to store or process data.

8.10 **Information Asset Owners (IAO) and Information Asset Administrators (IAA)**

The IAOs supported by the IAAs are the key backbone of our layered protection of personal data within NIFRS. Full detailed instructions of their responsibilities are contained within the IM Assurance Framework. In brief, however, they are primarily responsible for the daily monitoring and assurance of all NIFRS data sharing activity. They observe, monitor and report on the activity in their area to the SIRO at set intervals and provide formal assurance to the SIRO and NIFRS Board via the IM SharePoint site.

8.11 **All Staff**

It is the responsibility of all staff to process information in accordance with data protection laws and to adhere to the policies, procedures and guidance that are laid down by NIFRS. Staff must protect the personal information held by NIFRS and take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. This is further enforced by the common law duty of confidentiality that binds all public sector employees.

In addition, all staff have a responsibility to ensure that any information they supply to NIFRS in connection with their employment is accurate and up-to-date, for example, change of address (SC45) and name (SC45a). They should also check any information that NIFRS may send out from time to time which gives details of information that is being held and processed about them and inform the HR Employee Services Team immediately if any of the details are incorrect. NIFRS cannot be held accountable for errors arising from changes about which it has not been informed.

9 PRIVACY NOTICE

9.1 A Privacy Notice will let individuals know how NIFRS uses their personal information.

9.2 Under the GDPR NIFRS has a legal duty to protect any information collected from you and adheres to strict security standards to prevent any unauthorised access to it.

9.3 Should NIFRS wish to use information collected for a purpose other than the purpose for which it was originally collected or to disclose information to a third party, they may be allowed if it is fair to the individual to do so and this change of use or exchange has been agreed with the Information Security Manager. However, if we intend to make a significant change to how we use or process the information the individual's consent is required.

10 DATA SECURITY

10.1 The need to ensure that personal data is kept securely means that appropriate technical and organisational measures must be taken to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

10.2 Personal information must not be disclosed either orally, in writing or by any other means to any unauthorised third party. By far the most common cause of this is sending data to the wrong recipient either by post or by email.

10.3 All data that is held by NIFRS should be on secure servers or secure locations, with access restricted to selected members of staff.

10.4 The security of servers and data locations should be reviewed periodically by the Head of Information Technology in line with the IS/IT Policy.

10.5 The IM Assurance Framework provides detailed instruction for all NIFRS departments as to their requirements to adequately map and record all data transfers and usage. Without adequate knowledge of what we as an organisation are doing we cannot adequately protect the data in our control. This is again primarily achieved by the use of the NIFRS IM SharePoint site.

10.6 Extensive guidance on the practicalities of how best to protect all data in our possession, be it physical or electronic, is contained within the IM Assurance Framework and the supporting NIFRS IM Guides.

11 CCTV CAMERAS

11.1 NIFRS has a separate specific CCTV Policy which closely controls the use of CCTV within the organisation.

11.2 NIFRS operates a number of CCTV Cameras at various locations, and in doing so, must comply with its obligations under GDPR. The purpose of the cameras is as follows:

- To prevent & detect crime and anti-social behaviour; and
- To ensure public health & safety.

11.3 The Information Security Manager, acting on behalf of the SIRO, maintains day-to-day responsibility for the management of all CCTV across the NIFRS estate including that mounted on the Command Support Units, Area Ladder Platforms and Body Worn Video.

12 PHOTOGRAPHS

12.1 Before taking photographs or videos, consideration must be given as to whether consent is required and the decision documented. The Photography & Video Consent form from the Corporate Communications Department should be completed if consent is required.

12.2 Service issue devices are the primary authorised method of capturing images. On occasions, other sources may be used and acknowledged.

12.3 Corporate Communications will approve all photography and videos issued to media outlets. Social media contributors are responsible for photographs/images that they post or share on their social media platforms – if in doubt about what can be posted or shared, advice should be sought from Corporate Communications.

12.4 Personnel are advised that it is forbidden, even with a personal device, to take inappropriate photographs/videos whilst on duty. This includes, but is not

limited to, photographs of colleagues without their knowledge, photographs of members of the public or children without appropriate consent. This does not, however, inhibit taking of photographs which are to be used to substantiate issues being raised through the Fraud or Whistleblowing Policies or the investigation of same. Data Protection considerations should be taken into account when taking images to ensure that no personal data is inadvertently captured. Images taken should only be retained for the agreed purpose and should be disposed of in a secure and timely manner.

12.5 Contractors should be advised that the use of photography should be limited. Data Protection considerations should be taken into account when taking images to ensure that no personal data is inadvertently captured. Images taken should be retained for the agreed purpose and should be disposed of in a secure and timely manner.

12.6 NIFRS will hold photographs and videos for 5 years. After this date they will no longer be used by NIFRS but may be passed to the Public Records Office Northern Ireland if they are of historical value.

13 DISCLOSURE OF PERSONAL INFORMATION & DATA SHARING

13.1 NIFRS applies strict conditions with respect to the disclosure of personal information both internally and externally. Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

13.2 Sensitive and personal data will not normally be passed to organisations outside NIFRS, except where an organisation may have a legal and legitimate reason for access and a requirement for the data in order to carry out its function, eg, National Fraud Initiative, law enforcement, prosecution, child protection – this list is not exhaustive. If personal information is given to another organisation or person outside of the Service, the disclosing person must identify the lawful basis for the disclosure (see section 7 above) and

record their reasoning for using this basis. This record as a minimum should include:

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

13.3 Organisations wishing to have access to named, sensitive or personal data must be directed to the Personal Data Guardian and either:

- provide a suitable Information or Data Sharing Protocol which NIFRS is willing to sign up to; or
- sign up to NIFRS Information or Data Sharing Protocol before any data is released.

If an Information or Data Sharing Protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will provide the legal basis for disclosure.

No personal data, with the exception of data provided to comply with the National Fraud Initiative (NFI), should be released by any staff member without discussion with and the approval of the Personal Data Guardian.

13.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

13.5 When personal information is given either externally or internally, it must be communicated in a secure manner. For external communications use a secure communications system, special delivery or courier, etc. For internal communications either hand deliver or make sure you email the information to the correct recipient.

14 NATIONAL FRAUD INITIATIVE

14.1 NIFRS participates in a biennial National Fraud Initiative (NFI) exercise initiated by the Comptroller and Auditor General under Statutory Provisions contained in Articles 4A to 4H of the Audit and Accountability (Northern Ireland) Order 2003 as inserted by the Serious Crime Act 2007. Under these provisions, NIFRS will share information with other bodies responsible for auditing or administering public funds in order to prevent and detect fraud.

14.2 The data requirements of the NFI and the use/exchange of information have been approved by the Data Commissioner and the process does not require, under the terms of data protection laws, the consent of the individuals concerned.

15 SUBJECT ACCESS REQUESTS

15.1 Individuals whose personal data is held by NIFRS are entitled to:

- ask what information NIFRS holds about them and why;
- ask how to gain access to it; and
- be informed of how to keep it up-to-date and given the opportunity to amend this if it is incorrect.

15.2 The process for dealing with requests for personal information is outlined at Appendix E.

15.3 We will process your request as quickly as possible but you should be aware that the legislation allows NIFRS **one month** to respond to your request; however, if the request is complex an additional 2 months will be permitted.

15.4 If you feel that NIFRS has failed to respond correctly to your request for information you have the right to seek a review in the first instance with NIFRS Senior Information Risk Owner (SIRO) – by email to: siro@nifrs.org

15.5 Alternatively, the data subject may complain directly to the Information Commissioner's Office (ICO). NIFRS will inform all applicants of their right to complain to the ICO in responding to all requests for information. Information Commissioner's Office, 3 Floor, 14 Cromac Street, Belfast, BT7 2JB, website: www.ico.gov.uk

15.6 In relation to data portability NIFRS will provide the data requested in a structured, commonly used and machine readable format. This will be either to the individual who has requested it or to the Data Controller they have requested it to be sent to.

16 TRANSFER OF DATA OUTSIDE UK

16.1 It may sometimes be necessary to transfer personal information overseas. When this is needed, information can only be shared within the European Economic Area (EEA).

16.2 Any transfers will be made via the Information Security Manager and in full compliance with all aspects of the law.

17 PROTECTIVE MARKED DATA

17.1 Some data held by NIFRS may be deemed sensitive in terms of National Security and whilst data exchanges of this type are minimal, and are highlighted and controlled using the Protective Marking System, it is important that this data is held securely and that checks and balances exist.

17.2 Data exchanges of this nature are managed by the NIFRS Information Management Lead and will be managed in line with government guidelines on this matter. Only staff members with sufficient clearance will be permitted access to this data and it is the responsibility of the Information Management Lead to ensure that the data is controlled.

18 SECURITY VETTING

18.1 Data obtained through the security vetting process will be managed in accordance with GDPR principles and overseen by the Personal Data Guardian.

19 THIRD PARTY USERS OF PERSONAL INFORMATION

19.1 Any third parties who are users of personal information supplied by NIFRS will be required to confirm and demonstrate that they will abide by the requirements of GDPR. There will be an expectation that these parties will audit their compliance with GDPR and provide written assurances to NIFRS in this respect. NIFRS will retain the right to inspect and oversee the use of this data by third party users. The SIRO will ensure that this occurs as part of the IM Assurance Framework.

19.2 NIFRS must be notified without undue delay of any breaches of NIFRS personal information used by third parties.

20 CONTRACTS

20.1 NIFRS Contracts must comply with the standards set out by the ICO and must set out the subject matter and duration of the process, the nature and stated purpose of the processing activities, types of personal data, categories of data subject, and the obligations and rights of the controller.

At a minimum, NIFRS contracts must include terms that specify:

- Acting only on written instruction;
- Those involved in processing the data are subject to a duty of confidence;
- Appropriate measures will be taken to ensure the security of the processing;
- Sub-processing will only be engaged with the prior consent of the controller and under a written contract;

- The controller will assist the processor in dealing with Subject Access Requests and allowing data subjects to exercise their rights under GDPR;
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments;
- Delete or return all personal data at the end of the contract;
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and the processor to meet their legal obligations; and
- Nothing will be done by either the Controller or the processor to infringe on GDPR.

21 ACCURACY & RELEVANCE

21.1 It is the responsibility of those who receive personal information to make sure, so far as is possible, that it is accurate and up-to-date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up-to-date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

21.2 'Data subjects' have a right to access personal information held about them and have errors corrected. More information about a 'data subject's' rights can be found in section 22 of this Policy.

22 POLICY BREACHES

22.1 All breaches of the GDPR principles should be reported immediately to NIFRS Information & Security Manager on 028 9266 4221.

22.2 The Information Commissioner's Office has the power to take regulatory action against public bodies for breaches of GDPR, which includes monetary penalties, issue of an Undertaking or Enforcement Notice, criminal prosecution of organisations or the prosecution of individuals.

22.3 Failure to comply with this Policy may result in disciplinary action under NIFRS Disciplinary Policy & Procedure.

23 RETENTION & DISPOSAL OF INFORMATION

23.1 NIFRS holds a large amount of personal information. The GDPR requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other reason for holding it.

23.2 The Information Retention Schedule must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively, advice should be sought from the Information & Security Manager.

24 INDIVIDUAL RIGHTS

24.1 Individuals have a number of rights under GDPR. These include:

- The right to be informed – See section 5 - Collecting Personal Information;
- The right to access – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- The right to rectification – Personal data can be rectified if it is inaccurate or incomplete;
- The right to erasure – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing;
- The right to restrict processing – Person has the right to block or suppress processing of their personal data;
- The right of data portability – Allows a person to obtain and re-use their personal data for their own purposes;
- The right to object – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical research and statistics; and

- Rights related to automated decision making/profiling – A person can ask for human intervention in an automated process.

24.2 If any department or Station receives such a request on any of the above matters they should seek advice from the Information & Security Manager.

25 DATA PROTECTION TRAINING

25.1 All individuals permitted to access personal data in line with their work duties will be trained in the requirements of the Data Protection Policy and related Procedures and will undertake any relevant training that may be appropriate and deemed necessary by NIFRS.

25.2 Data Protection Training will form part of NIFRS' induction for new employees.

26 EQUALITY

26.1 NIFRS is committed to equality of opportunity for all employees and service users. This Policy will be reviewed periodically in accordance with Section 75 equality obligations and best practice and also with regard to NIFRS statutory obligations to make NIFRS corporate publications and information accessible in alternative formats, where reasonable.

27 REVIEW & REVISION

27.1 The Policy has been screened and consulted upon under NIFRS Section 75 Statutory Equality obligations.

27.2 In line with the Policy Development Framework the Planning, Performance & Governance Function will review this Policy every 3 years or sooner should legislation change.

28 FURTHER INFORMATION & GUIDANCE

28.1 Further information and guidance on Data Protection in NIFRS and this Policy can be obtained from:

Information & Security Manager
Northern Ireland Fire & Rescue Service
1 Seymour Street
Lisburn
BT27 4SX

28.2 Further information and guidance on ICT Security can be obtained from:

Head of Information Technology
Northern Ireland Fire & Rescue Service
1 Seymour Street
Lisburn
BT27 4SX

APPENDIX A

THE 6 PRINCIPLES OF GDPR

As Data Controller, NIFRS must be accountable and keep records evidencing our compliance with the following GDPR principles. Such record keeping will include the logging of any new systems onto our Information Asset Register and updating as necessary, information flow and record management registers.

1 Lawfulness, Fairness and Transparency

Personal data can only be processed if there is a lawful reason for doing so. It must be fair to the data subject and you must be fully transparent with the data subject as to why you are collecting their data and how it is going to be used and shared.

2 Purpose Limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, although further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted in certain circumstances.

3 Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4 Accuracy

Personal data must be accurate and, where necessary, kept up-to-date.
Where personal data is inaccurate every reasonable step should be taken to enable its deletion (where appropriate) or correction without delay.

5 Storage Limitation

Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary. Such personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in certain circumstances and subject to the implementation of the appropriate technical and organisational measures.

6 Integrity and Confidentiality

Personal data must be processed in an appropriately secure manner including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

APPENDIX B

GDPR Article 6 and Article 9

Article 6 Conditions – Personal Data

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.**

Article 9 Conditions – Special Category Data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

APPENDIX C

DATA PROTECTION DEFINITIONS

Personal Data means data (manual or electronic) which relates to a living individual who can be identified, either by the data alone or with other information or opinion held by the data controller.

Data means information about individuals which is being processed automatically or is recorded with the intention of being processed automatically. Any data recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system.

Data Subject means any individual who is the subject of personal data.

Data Controller means a person who determines the purpose for which and the manner in which any personal data is, or is to be, processed. For the purpose of this Procedure NIFRS is the data controller.

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Processing means obtaining, recording or holding the information or amending, adding to, deleting, disclosure, or destruction of the information or data.

Sensitive Category Data means personal data consisting of information as to an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); physical or mental health condition; genetic or biometric information; sexual orientation; commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in such proceedings.

Sensitive personal data is that because information about these matters is likely to be of a particularly sensitive nature it needs to be treated with greater care than

other personal data. The loss, theft or mishandling of sensitive personal data is likely to be of a greater detriment to the individual than the loss, etc, of other personal data. Sensitive category data must be processed fairly, lawfully and in accordance with the requirements of GDPR. The nature of the data is also a factor in deciding what security measures are necessary to protect the information.

Information Commissioner's Office means the Office appointed to regulate and oversee the implementation of GDPR and other related legislation.

Subject Access Request (SAR) means formal written or email request received from the data subject for sight or a copy of their data/record(s) held by the Organisation.

APPENDIX D

GDPR EXEMPTIONS

The primary exemptions concerns:

- National Security;
- Defence;
- Public Security;
- The prevention, investigation, detection or prosecution of criminal offences;
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- The protection of judicial independence and proceedings;
- Breaches of ethics in regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others; or
- The enforcement of civil law matters.

APPENDIX E

SUBJECT ACCESS REQUEST FLOWCHART

Process to be followed for Employees requesting Access to Personal Files

As normal course of business, employees are permitted to have access to their personal file within the designated office where personal records are kept and maintained. All individual requests must be made in writing on a PF5 form, stating the reason to the Area Commander/PO Grade Head of Department/HR Employee Services Team, HQ. See Guidance on Management of Personal Files on the Global Folder/DMS.

Arrangements will be made to allow the employee to view their file within a reasonable period and in the presence of a designated Officer.

No information may be altered or removed but the employee can obtain copies of information.

On receipt of the requested information employees will be required to complete an Information Receipt Form (PF6).

Process to be followed on receipt of a Request from an Individual for Personal Information (Data Subject)

Submit a Subject Access Request to NIFRS Information Security Manager - NIFRS HQ.

The request must be: In writing and specify the personal information required giving as much detail as possible to enable it to be located. Employee access to other personal information not normally held on a personal file must be requested by completing a Subject Access Request. If necessary, clarification will be provided by the ISM.

A written acknowledgement of the request will be issued by the Information Security Manager.

If further information is required to clarify the request, the Information Security Manager may issue a Subject Access Request form (SC87), it may also be necessary to contact the person by phone or letter.

Once the requested information is available, you will be contacted **within 1 month** to make arrangements for its collection. If it is not possible for you to attend a specific location, alternative arrangements will be made to enable you to access/collect the information.

If you feel that NIFRS has failed to respond correctly to your request for information, you have the right to seek a review in the first instance with NIFRS Senior Information Risk Owner (SIRO) – by email to: siro@nifrs.org

Alternatively, the data subject may complain directly to the Information Commissioner's Office (ICO). NIFRS will inform all applicants of their right to complain to the ICO in responding to all requests for information.

APPENDIX F

DATA PROTECTION REPORTING FLOWCHART