NORTH YORKSHIRE
FIRE & RESCUE SERVICE

Data Protection Policy

North Yorkshire Fire & Rescue Service
Headquarters
Alverton Court
Crosby Road
Northallerton
North Yorkshire
DL6 1FE

Tel: 01609 780 150

www.northyorksfire.gov.uk

TABLE OF CONTENTS

DOCUMENT CHANGE HISTORY

Date	Version	Status	Author	Details of Change
10th October 2014	0.1	Draft	CAO Manager	Initial Document
02nd February 2015	1.0	Approved	CAO	Published
10th October 2016	2.0	Approved	CAO Manager and I G Officer	Not full review - inserted 4.12 due to introduction of information security incident management procedure.
27th January 2017	3.0	Approved	CAO Manager and Information Governance Officer	Full review. Amended appendix with information security incident management procedure. Role title changed and included example of Schedule 2 and 3 conditions that need to be met. To be updated in 2017/18 for implementation of GDPR.
13th April 2018	3.1	Draft	CAO Manager and IG Officer	Full review and update to align with GDPR
2nd May 2018	4.0	Approved	IGG	Reviewed & approved
22nd May 2018	4.1	Draft	CAOSI Lead	Amendment to DPO contact details
5th March 2021	4.2	Draft	CAO Manager	Amendment to HQ address
9th May 2022	4.3		DPO	Full Review - Amended Introduction and included links to relevant policies and procedures. Responsibilities and contact details updated. Section 5.6 employee data removed as this content is covered elsewhere in the policy. Further consent details and conditions provided.
7th June 2022	5.0	Approved	Info Management Lead	Reviewed & approved.

This is an electronic version of the approved version; paper copies are only valid as of the last update. Please refer to the master copy or the document author if you are in any doubt about the document content.

Policy Superseding:

This policy supersedes the following policies from the date adopted date in the information panel:

- Data Protection Policy

Contributors:

Development of this policy was assisted through information provided by the following organisations:

- Information Commissioner's Office Website http://ico.org.uk/

1. INTRODUCTION

North Yorkshire Fire and Rescue Service (the Service) is committed to ensuring that the workforce undertake their legitimate duties in a manner that is compatible with the data protection principles.

The Service recognises the sensitivity of processed personal information and its obligations in respect of data held by the North Yorkshire Fire and Rescue Authority (the Data Controller), specifically to protect individuals from harm caused by the use of inaccurate information of the misuse of correct information.

The Service also acknowledges the clear benefits of having accurate and up-to-date information available for use in an appropriate format, when and where it is required. A pragmatic approach to the application of the principles within the Data Protection Act 2018 will help to deliver these benefits. .

:

2. PURPOSE

In order to operate effectively, the Service, processes (collects, stores, shares and uses) information relating to individuals and organisations with whom we work. These may include members of the public, current, past and prospective employees, clients, customers, law enforcement agencies and other social agencies. It also gathers information relating to sites and premises within communities that it supports. In addition, the Service may be required by law to collect and process information in order to comply with the requirements of local and central government.

The purpose of the UK GDPR and The Data Protection Act 2018 is to regulate the way that personal data about individuals (held either electronically i.e. in computer records, e-mail, back-up/archive systems/ word processing documents, in a manual filing system, or gather by CCVT or other media such as audio or video recordings) is processed (obtained, stored, used, disclosed and destroyed). The Act incorporates the General Data Protection Regulation 2016 under Part 2 of the Act, and intends to protect the rights of living individuals when information is processed about them by organisations, including the Service.

3. SCOPE

This policy applies to any member of the workforce, be it staff, contractors, consultants, temporaries, and other workers at the Service including all personnel affiliated with third parties.

This policy should be given during the induction of new employees and to contractors prior to the commencement of work.

4. RESPONSIBILITIES

The Chief Fire Officer (as the data controller) is legally responsible for the Service's compliance with the DPA 2018.

Tactical Leadership Team (TLT) on behalf of the Authority is responsible for compliance with the GDPR and its principles and must be able to demonstrate compliance (accountability).

The Data Protection Officer (DPO) is responsible for overseeing compliance with the data protection legislation, including by ensuring the implementation of this and associated policies. .

The **Senior Information Risk Owner (SIRO)** is responsible for ensuring appropriate technical and/or organisational measures for the type of information (including personal data), together with any risks to information and the business. The SIRO has ownership of risk, ensures that information management and other risks are considered, understands how the strategic business goals of the Service may be affected by information system failures, and is supported by the Information Assurance resources and other stakeholders and subject matter experts in achieving compliance.
.

Information Asset Owners (IAO) must identify any personal data handling within their functions / sections; then implement and monitor appropriate data handling procedures that ensure employees comply with the data protection principles and individual's data rights. They also need to ensure that the processing of personal data is recorded on the Record of Processing Activity register.

All persons working for, or on behalf of, the Service, having access to personal data, are required to comply with the requirements of the DPA 2018. Every member of the workforce must process information in accordance with this Policy, Staff Code of Conduct and associated procedures and standards.

If employees have any questions about data protection in general, this policy or their obligations under it, they should contact theCompliance Team in the first instance.

Alternatively, the DPO can be contacted directly via the following:

Data Protection Officer
Joint Police and Fire Headquarters
Alverton Court
Crosby Road
Northallerton
DL6 1BF
Emaill: dataprotectionofficer@northyorkshirefire.gov.uk

5. POLICY

5.1 DEFINITIONS

To aid the understanding of this document and provisions of the Data Protection legislation the following definitions are provided:

Data Subject is the individual about whom the personal data is processed.

Personal data means any information relating to an identified or identifiable living natural person who can be identified, directly or indirectly by reference to an identifier such as a name, and identification number, location data, an online identifier, physical, psychological, genetic, mental, economic, cultural or social identity. Personal data includes facts, opinions or intentions relating to the individual; examples are:

- driving license number or vehicle registration mark
- Address,
- Date of birth,
- Martial status,
- Asset number of personal issued IT equipment

Special categories of personal data mean personal data consisting of information relating to the data subject's:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership;

- Health;
- Sexual life / sexual orientation;
- Genetic or biometric data.

Data Controller means the Chief Fire Officer of North Yorkshire Fire and Rescue Authority as the organisation that determines (alone or jointly) the purposes for which and the manner in which personal data is processed.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, such as:

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Processor means any person, other than an employee of the Authority, who processes personal data on behalf of the Data Controller, e.g. an organisation contracted to provide a payroll service, or identification cards.

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

Third party means a person, public authority, agency or body other than the data subject, controller, processor and who, under the direct instruction of the controller or processor, are authorised to process personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be valid, it must be withdrawable and it must not be a condition of the data subject accessing a service.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the data subject’s health status;

Binding corporate rules means personal data protection policies that are adhered to by a controller or processor.

The **Information Commissioner’s Office (ICO)** undertake the role of **'supervisory authority'** they are an independent authority which is set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO investigate high risk personal data breaches and contraventions

of the data protection legislation. The ICO have enforcement powers such as issuing of fines, serving information notices or conducting audits, to ensure compliance with the data protection legislation.

5.2 DATA PROTECTION PRINCIPLES

The Act sets out principles for good information, handling and processing, a full description of each can be found within the ICO's guide to the GDPR principles . These principles are legally enforceable by the ICO and courts, and require that personal data is:

1. Processed lawfully, fairly and in a transparent manner
2. Obtained and used for specified and lawful purposes
3. Adequate, relevant and limited to what is necessary for the purpose
4. Accurate and, where necessary kept up to date
5. Not kept in an identifiable form for longer than necessary
6. Processed in a manner to ensure security, using appropriate technical and organisational measures

A number of offences have been established by the Act. Misuse of personal information could result in a conviction and a fine. It is important that staff understand that they may be committing an offence if they misuse information.

5.3 MEETING THE PRINCIPLES

The Service will ensure that it has identified an appropriate legal basis to process personal information and that the processing is reasonable and proportionate to the aim pursued.

Where required, all individuals whose details are processed by the Service will be informed why and the way in which their data will be obtained, held, used, and disclosed and their data protection rights, by means of a privacy notice.

Data collected will be limited to what is necessary to meet the purpose and only to the extent that is needed to perform Service functions, meet legal and regulatory requirements, and employment obligations. The Service will not collect data for the 'just in case' scenario or use data for an incompatible purpose once collected.

The data collected will be accurate, and where necessary kept up to date. It will be held securely and accessed by individuals only for the intended purposes.

Data will only be kept for as long as necessary to meet the purpose and in accordance with the Retention Schedule. Where it is necessary to only keep the non-personal data, arrangements will be put in place to delete the personal data.

To assist monitoring of compliance, the governance of information is included within the Watch Performance Audits and Information Governance Boards are maintained at every location. Compliance checks undertaken by the Compliance Team may also be undertaken.

5.4 LAWFULNESS OF PROCESSING

The Principal purposes for which the Service processes information are:

- Administration of the Service and its workforce (e.g. employment, HR, Payroll purposes under any of the following Health and Safety at Work Act 1974 and Management of Health and Safety at Work Regulations 1992, the Fire Services (Appointments and Promotion) (England and Wales) Regulations 2004, Section 112 of the Local Government Finance Act 1988);.
- Safeguarding (Safe and Well/Fire Safety visits conducted under Fire and Rescue Services Act 2004 to meet obligations such as promoting fire safety, reducing risks from fire, providing advice on actions to take in the event of a fire, safeguarding by improving safety and providing support to improve health and wellbeing);
- Conducting Fire Investigations under Sections 45-48 of the Fire and Rescue Services Act 2004 (duty to protect life and property from fire);
- Rendering assistance to the public in accordance with policies and procedures

The principal purpose for which the Service processes information is to improve accountability within the Service and ensure that the Service is combating issues important to the community. Information is also processed for purposes relating to the use of CCTV systems for crime prevention.

Personal data shall not be processed (including disclosure) unless at least one of the conditions in Article 6 of the GDPR is met and in the case of the processing of special categories of personal data at least one of the conditions in Article 9 of the Regulations must also be met. Where Article 9 is being relied on, we must also meet at least one Condition in Schedule 1 of the Data Protection Act 2018 to ensure the processing is lawful.

For example, for criminal conviction data or data about offences, both an Article 6 condition and an additional condition under Article 9 as set out in the UK law needs to be met. At least one Schedule 1 Condition must also be met and documented.

One of the conditions to process personal data is consent, which must be freely given. The GDPR recognises that public authorities and employers will rarely be able to rely on consent as a lawful basis due to the clear imbalance between the individual and the public authority / employer, as it's unlikely that consent can be freely given in all the circumstances of a specific situation. Where we rely on consent, business areas must ensure they have a process in place to record that explicit and informed consent

has been given, to review the validity of consent (where appropriate) by way of a consent audit, and to allow the withdrawal of consent either by deleting the personal data or anonymising it to remove any personal identifiable information. Processing based on consent must be documented on the Consent Register held by the Compliance Team.

The majority of the remaining conditions require the processing to be 'necessary', therefore the processing must be a targeted and proportionate way of achieving the purpose. It would not be necessary if the purpose could be reasonably achieved by a less intrusive way.

The Service must determine a lawful basis before it begins processing; therefore employees must seek the **DPO's** advice when determining the relevant condition to process personal data, as consideration will have to be given to associated data protection requirement under the Data Protection Act, such as requirements for a Data Protection Impact Assessment (DPIA), updating of privacy information, consideration of the need for a Data Processing Contract or Information Sharing Agreement to be put in place. There will also be a requirement to update the Record of Processing register.

Appendix A provides the Article 6 and 9 conditions.

5.5 RIGHT TO BE INFORMED - PRIVACY NOTICES

The right to be informed encompasses an obligation to provide individuals, including employees, information about how the Service will use their personal data, including the lawful basis for processing. This is provided to individuals in a form of a 'Privacy Notice'.

This right applies whether the Service collects the personal data directly from the individual or another source.

If data is provided to the Service by another source, the Service must provide a privacy notice within one month of obtaining the data, unless the individual already has the information or an exemption applies.

A privacy notice must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child;
- Include the right to withdraw consent if the processing was based on consent, and;
- Include all the information within either Article 13 or 14 of the Regulation.

Privacy Notices are published on our website here: What are you doing with my personal information and include areas like:

- Staff
- Recruitment

- Youth working
- Website and social media
- Technical Fire Safety Audits and SSRI
- Safe and Well
- Home Fire Safety Visit
- Fire Investigation
- Emergency Incidents
- CCTV

The Service issue a 'How information about you will be used' at the beginning of Home Fire Safety Visits and recipients of Safe and Well Visits receive the information within the Safe and Well booklet. Recruitment documentation and Technical Fire Safety Audit correspondence include a link to the relevant website privacy notice.

The Compliance Team will continue to develop relevant practices to ensure that privacy notices are appropriately given, dependant on the circumstances. Should the way in which information is processed change, or new initiatives be pursued, the Compliance Team must be consulted by the relevant IAO to ensure that privacy notices are kept up to date. The IAOs should review their privacy notices at least annually to ensure they are still up to date, and advise the Compliance Team of any changes required

Privacy Notices are required in most circumstances, the **Compliance Team**, will support the production of privacy notices, taking into consideration how it should be provided to the individual and advise when one is not required.

5.6 DATA PROTECTION RIGHTS

The Regulation grants several rights to individuals. Not all of them are absolute and can be subject to exemption. They are, the right:

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- Not to be subject to a decision based solely on automated processing, including profiling

The **DPO's** advice must be sought where a decision is going to be made based solely on automated processing, including profiling, as this is prohibited by the Regulation in certain circumstances and appropriate safeguards need to be put in place. This includes the requirement to notify the individual of such processing, so they can exercise the right to obtain meaningful human intervention (someone who has authority to change the decision), express their views, obtain an explanation of the decision reached and contest the decision.

Where data is being processed by the Service and the identity of the individual has been confirmed, the Service shall respond to the rights request and provide the data subject with a response.

The Data Subject Rights Request Procedure provides detailed guidance on how requests will be dealt with, including the statutory timescales for a response to be provided.

All requests received (verbally, electronically or in writing) should be forwarded immediately to the **Relevant Team** to deal with; Subject Access Requests and disclosure requests should be dealt with by the Civil Disclosure Team; Rectification and Erasure requests will be dealt with by Records Compliance, and any other Requests should be forwarded to the DPO.

5.7 THE DATA PROTECTION OFFICER

The DPA 2018 introduces a duty upon the Service to appoint a Data Protection Officer (DPO) to oversee compliance with the Regulation and at least to:

- Inform and advise the Service and employees who carry out processing of their obligations pursuant to this Regulation and to other data protection provisions;
- Monitor compliance with this Regulation, with other data protection provisions and with the policies of the Service in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Provide advice where requested as regards the data protection impact assessment and monitor its performance;
- Cooperate with the ICO;
- Act as the contact point for the ICO on issues relating to processing, including the prior consultation on data protection impact assessments, and to consult, where appropriate, with regard to any other matter.

5.8 RECORD OF PROCESSING ACTIVITY REGISTER

It is a legal requirement that the Service maintains a register of all the personal data that it processes.

The Compliance Team maintains this register which includes, but not limited to, the legal basis for processing personal information, the processing purpose, who it is shared with, retention and categories of personal data.

All processing of personal data must be recorded on the register, and be provided to the ICO upon request.

5.9 DATA PROCESSORS

To ensure compliance with the requirements of the legislation in respect of processing carried out on behalf of the Service, by another body (data processor), the Service will only use processors providing sufficient guarantees, in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of the data protection legislation, including for the security of processing. The Information Security Officer, within the Compliance Team, will advise on the necessary security baseline practices which any prospective supplier must meet to ensure adequate safeguarding of the data we are responsible for.

The processing by a processor shall be governed by a contract. The contract must stipulate the requirements set out within Article 28 of the GDPR, including but not limited to:

- The subject-matter and duration of the processing
- The nature and purposes of the processing
- The type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject.
- Ensuring that they and all of their staff, who have access to personal data, are aware of this policy and are aware of their duties and responsibilities under the Regulations.
- Allow data protection audits by the Service of data held on its' behalf (if requested)
- Confirm that they will abide by the requirements of the Regulations

After the completion of processing on behalf of the Service, a processor should, at the choice of the Service, return or delete the personal data, unless there is a requirement to store the personal data.

Advice must be sought from the **DPO** prior to any engagement with a data processor to ensure the contractual arrangements meet the legislative requirements. The

Service continues to work with all existing data processors to update contracts in accordance with the Procurement Policy Note 03/17.

5.10 DATA PROTECTION BY DESIGN

The DPA 2018 makes privacy by design a legal requirement, under the term 'data protection by design and by default'. This is an approach that promotes privacy and data protection compliance in everything we do, and to be considered particularly at the beginning of a project.

The Service will ensure that the data it collects and uses is proportionate and necessary for the intended purpose. That the processes, procedures and systems enable the data to be accessed only by those that require access and deleted in accordance with the retention schedule.

The Service will demonstrate transparency in accordance with the Regulation and look at creating and improving security features on an ongoing basis.

The undertaking of Data Protection Impact Assessments prior to any processing commencing will assist the Service comply with this requirement.

You should consider data protection and privacy particularly when working with personal data in the following scenarios:

- New technologies – processing involved in the use of new technologies or the novel application of existing technology (including artificial intelligence);
- Denial of service – decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data;
- Large scale profiling – any profiling of individuals on a large scale;
- Biometrics – any processing of biometric data including fingerprint log ins to assets or voice recognition software;
- Genetic data – any processing of genetic data, other than that processed by an individual GP or health professional for the provision of heath care direct to the data subject e.g. fitness test results;
- Data matching – combining, comparing or matching personal data obtained from multiple sources;
- Invisible processing – processing of personal data that has not been obtained direct rom the data subject in circumstances where the controller considers that compliance with Article 14 of the UK GDPR would prove impossible or involve

disproportionate effort i.e. we can not reasonably contact individuals to let them know we are processing their personal data;

- Tracking – processing which involves tracking an individual's geolocation or behaviour, including but not limited to, the online environment;
- Targeting of children or other vulnerable individuals – the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if it is intended to be used to offer online services to children;
- Risk of physical harm – where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of an individual;
- Automated decision-making – with legal or similar significant effect based on personal data;
- Systematic monitoring – facilitated by use of personal data;

Evaluation or scoring – based on personal data e.g. employment assessments, recruitment criteria scoring

5.11 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is required in situations where data processing is likely to result in high risk to data subjects' rights and freedoms. DPIAs take a systematic approach to analysing the process, data flows and risks associated with the collection of personal data, and impacts on privacy. It is best practice to incorporate the assessment at the outset of a project as this allows for early intervention on any risk identifies with the proposed methods of collection and processing of data. It also permits departments to address issues associated with misusing personal data.

The DPIA enables the Service to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individual's expectations of privacy and help avoid reputation damage which might otherwise occur.

A DPIA must:

- Describe the nature, scope, context and purposes of processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks

Risks will often arise by processing:

- Inaccurate, insufficient or out of date data;
- Gathering and retaining excessive or irrelevant data;
- Keeping data for longer than is necessary;
- Disclosing data to third party individuals/organisations without consent of the data subject;
- Processing the personal data of an individual in ways that are unacceptable or unexpected;
- Not storing the data securely or sharing data securely.

The Compliance Team and, where appropriate, individuals and relevant experts must be consulted on completion. Data Processors can be requested to assist with the completion. The DPO will ensure the DPIA meets the required standard and once a completed DPIA has been signed off, a published version will be made available to everyone in force. However, data protection and privacy will need to be considered throughout a project's lifespan, especially if changes are required, as new locations, new technologies or additional data could be collected and introduce risk.

If a DPIA indicates that the data processing is high risk and the Service cannot sufficiently address those risks, the DPO mayl be required to review and approve that the processing operation complies with the legislation. Where high risks cannot be mitigated, the initiative may need to be abandoned or the ICO consulted for further guidance and approval of the intended processing.

The Service will ensure that DPIA are undertaken at the earliest opportunity where required. Information Asset Owners should consult the DPIA Standard Operating Procedure and Business Management Framework for further guidance.

5.13 INTERNATIONAL TRANSFER

The data protection legislation imposes restrictions on the transfer of personal data outside the European Economic Area to third countries or internal organisations.

Personal data may only be transferred outside the EEA in compliance with the conditions for transfer set out within the Regulation. Specifically, transfers must be based on an adequacy decision or where this is not possible, under Standard Contractual clauses or in rare circumstances, based on the assessment of the receiving party bring able to securely process the data.

The international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions was adopted by the Parliament in 2022 and can be used immediately.

No employee is to transfer Service data outside the EEA, for example, sending a work email to an organisation or individual outside the EU, logging on to work emails when outside the EU, or storing information on the cloud rather than internal servers, without consulting the Compliance Team to ensure the appropriate safeguards are met and adhered to.

The Service have opted for a UK based email service, however technical support may be provided by countries outside of the EU and therefore, email data may be transferred accordingly. Such data transfers are protected by European Commission (EC) Model clauses, meeting both the EC and Information Commissioner's Office requirements for providing adequate safeguards for the protection of individual's personal data.

5.13 SECURITY

The data protection legislation requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All employees have a responsibility to take appropriate technical and organisational security measures to safeguard personal information.

In particular, an employee should as a minimum ensure that:

- Paper files and other records or documents containing personal / special category data are kept in a secure environment, by locking them away in a secure cabinet
- Use the confidential waste bins to dispose of personal data
- Personal data held on computers and computer systems is protected by the use of secure passwords
- Computer networks that hold personal data will be protected with appropriate levels of physical and logical security to prevent access to that data by unauthorised parties
- Individual password should be such that they are not easily compromised

- The secure email system used, where appropriate, and apply the correct security markings for the transmission and receipt of emails to a trusted source. Refer to Protective Security Marking Policy and Information Handling Procedure
- Never upload or save any data off the Service's secure network

Employees should not remove information from a place of work unless it is absolutely necessary to do so; therefore there will be limited circumstance where an employee takes records off site containing personal data to enable them to do their role. If they do they must ensure that it is adequately protected from unauthorised use or disclosure. They must not leave their laptop, other device or any hard copies on the train, in the car or any other public place. They must also take care when observing the information in hardcopy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

Any loss of personal data must be reported in accordance with the Information Security Incident Management Procedure.

If an employee acquires any personal information in error, by whatever means, they shall report and manage it in accordance with the Information Security Incident Management Procedure.

5.14 REPORTING AN INFORMATION SECURITY INCIDENT

All employees have a responsibility to report any potential, suspected or actual data security incident immediately to the **Compliance Team** via the ITSS Helpdesk (out of hours Control), or direcrtly to the Team via a phone call or email, in order that all necessary and appropriate action can be taken.

If it is determined that the incident is a breach and results in a risk to an individual, the DPO or nominated representative will need to notify the ICO of the breach within 72 hours after having become aware if it.

If it is determined that the breach will likely result in a high risk to an individual, e.g. identity fraud, financial loss, sensitive data ending up in the public domain, the individual's safety being put in harm's way or a permanent change to their way of life, the individual must be informed without undue delay.

Further Information about what to do in the event of an information security incident can be found within the Information Security Incident Management Procedure.

An information security incident is an event that could breach our information security procedures. It may arise from (but not limited to):

- the loss or theft of data or information
- a deliberate attack on our systems
- the unauthorised or unlawful use of personal data by a member of staff
- misuse of information or equipment
- inappropriate disclosure
- accidental loss or equipment failure.

5.15 CONFIDENTIALITY

The Service will ensure that personal data is treated as confidential and access to personal data will be on a least-privilege, need to know, role requirement basis.

Employees during the course of employment may have access to, gain knowledge of or be entrusted with personal information, and or other confidential information. Employees are not to inappropriately disclose to any person or make any use of such information, in any form whatsoever, at any time, whether during or after the end of employment with the Service. Reference should be made to the Staff Code of Conduct.

However, employees need to be able to draw a distinction between ensuring personal data is treated as confidential, and the requirements of the Whistleblowing policy which provides avenues for staff to raise concerns as to malpractice or wrong doings. The Service expects the fullest co-operation of all its employees in securing the highest standards of service, and where employees are aware of or suspect malpractice, the Service will expect them to report these suspicions. Reference should be made to the Whistleblowing Policy.

5.16 DISCLOSURES

Release of information must be, and will be, in accordance with the provisions of the Regulations and associated data protection provisions. The Service has a duty to disclose certain data to public authorities and other agencies such as Her Majesty's Revenue and Customs (HMRC), Audit Commission, Her Majesty's Inspectorate of Constabulary (HMIC), internal and external auditors and the Coroner's Office. This will be carried out strictly in accordance with the statutory and other requirements.

5.17 SHARING

Disclosure of information amounts to processing under the data protection legislation. Therefore information shall not be disclosed unless an Article 6, and if special category personal data, Article 9 are satisfied (See 5.4).

There are occasions where the Service shares information. In all cases where information is shared the Service will have identified the lawful basis for disclosure, by having a legal obligation, vital, legitimate or public interest or having obtained the data subjects consent to share.

Where the Service share without asking the data subject, it must have a legal duty or power to share information with other statutory bodies from statute or from common law when the public interest is thought to be of greater importance than personal confidentiality.

Decisions will be made on a case by case basis, examples of this would be:

- disclosure is required by law (e.g. under an Act of Parliament creating a Statutory duty to disclose or a court order)
- for the detection, prevention and prosecution of crime or the apprehension of offenders;
- there is a public interest that outweighs the duty of confidence to the individual (e.g. health and safety);
- there is a risk of death or serious harm;
- in the substantial interest of the individual's health;
- in the vital interest of the individual concerned.

The Service are signatories to the North Yorkshire Multi-Agency Information Sharing Protocol. For regular sharing of information with third parties, the **Civil Disclosure Unit** must be contacted to assist with the development of an Information Sharing Agreement in accordance with the protocol.

5.18 TRAINING

The minimum training requirements for all roles across the organisation in relation to information governance and data protection is identified and recorded by the Data Protection Officer.

All employees are required to complete a Protecting Information Learn Pro module every two years, familiarise themselves with the content of the Information Governance Boards and digest the content of any Update Bulletin / Special Staff Newsletter communication.

The Service will continually review and update training materials to ensure appropriate role related training is given.

The Compliance Team will make available training and awareness communications which everyone working for the Service has a responsibility to familiarise themselves with.

5.19 INFORMATION COMMISSIONER'S OFFICE AND DATA PROTECTION FEE

All individuals have the right to lodge a compliant with the ICO in regards to the processing of their personal data or contact them to seek advice www.ico.gov.uk.

Annually the Service is required to pay a fee to the ICO, to ensure the continued funding of it. The Service is a Tier 3 organisation. The North Yorkshire Fire and Rescue Authority is registered with the ICO under reference: Z6875365.

5.20 CONSEQUENCES OF NON-COMPLIANCE

All employees are under an obligation to ensure that they have regard to the principles relating to the processing of personal data and this policy when collecting, accessing, using or disposing of personal information. Failure to observe the principles and this policy may result in an employee incurring personal criminal liability, or disciplinary action.

The ICO has powers, including the ability to fine organisations, to ensure that the principles as well as the rights of the individuals concerned are upheld according to the wording and the spirit of the Regulation.

If an employee is in any doubt about what they may or may not do with personal information, they should initially seek advice from their immediate manager, or contact the **Compliance Team.**

6. POLICY GOVERNANCE

The following table identifies who within North Yorkshire Fire & Rescue Service is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.

N.B Only **one** role is held accountable.

- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.

- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Tactical Leadership Team
Accountable	Chief Executive
Consulted	TLT, Unions
Informed	All Employees, All Temporary Staff, All Contractors, etc.

7. REFERENCES

The additional North Yorkshire Fire & Rescue Service service documents are relevant to this policy and are to be adhered to:

- Data Subject Rights Request Procedure
- DPIA Standard Operating Procedure
- Records Management Policy
- Information Handling Procedure
- Information Security and Handling Policy
- Protective Security Marking Policy
  -
  - Staff Code of Conduct
  - CCTV Scheme
  - Freedom of Information, Environmental Information Regulations Policy
  - Freedom of Information, Environmental Information Regulations Standard Operating Procedure
  - Information Handling SOP
  - ICT Assets Policy
  - ICT Security Policy
  - ICT Usage Policy
  - Visual Imaging Policy
  - Social Media Policy
  - Dealing with the Media SOP

Appendix A – Lawfulness of Processing

Article 6 states that processing shall be lawful only if at least one of the following applies:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purpose;

(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 or of another natural person;

(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 the controller or by a third party.

Article 9 states that processing of personal data revealing **special categories** of information is prohibited unless one of the following applies:

(a) the data subject has given **explicit consent** to the processing of the personal data for one or more specified purposes,

(b) processing is necessary for the purposes of carrying out the **obligations** and exercising specific rights of the controller or 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 and on condition that it will not be disclosed 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**, 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

(h) processing is necessary for the purposes of **preventive or occupational medicine**,

(i) processing is necessary for reasons of **public interest in the area of public health,** such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,

(j) processing is necessary for **archiving purposes in the public interest, scientific or historical research** purposes or statistical purposes in accordance with Article 89(1)