1142 Data Protection (and subject access requests)

The UK General Data Protection Regulation and the Data Protection Act 2018 (DPA) set rules to ensure personal information is handled correctly however it is collected, recorded and used (whether on paper, stored on computer, or recorded on any other material).

It also gives people rights over their personal data.

The Data Protection requirements apply to current, past and prospective contacts including employees, suppliers, clients and members of the public.

This policy explains how the Service will comply with the Data Protection legislation.

Knowledge of this policy and supporting procedures will enable employees to meet their responsibilities and comply with the Data Protection requirements.

OWNER	**Data Protection Officer**
LAST REVIEW	**June 2021**
REVIEW DUE DATE	**June 2023**
VERSION CONTROL/AMEND SCHEDULE	**11.0 – updated to reference 'UK GDPR'**

CROSS REFERENCES
Information Commissioner Guidance
Data Protection Act and Codes of Practice
Service Information and Security policies

CONTENTS

POLICY SECTION

1. Policy Statement

Cheshire Fire and Rescue Service will treat personal information lawfully and correctly in compliance with the Data Protection legislation (DPA) and any associated Codes of Practice.

The Service regards the proper treatment of personal information as very important to successful operations, and to maintaining confidence with employees, stakeholders and the public.

2. Specific Commitments

The Service will achieve good practice through adopting designated roles and responsibilities, implementing robust procedures, provision of training and appropriate controls. These actions will support all officers/staff to process information lawfully in accordance with the DPA, safeguarding personal data, and protecting the reputation of the Service.

The Service will implement procedures which ensure that the key Data Protection requirements are met, namely –

- To annually pay a fee to the Information Commissioner *(see Section 5)*,
- To process personal data in compliance with the six Data Protection principles and other requirements *(see Appendix 2)*,
- To comply with individuals' rights *(see Section 9)*.

3. Ownership/Monitoring

A senior officer (currently the Director of Governance and Commissioning) will hold specific responsibility for data protection in the organisation.

The Data Protection Officer is part of the Joint Corporate Services team. The Data Protection Officer (DPO) advises the data controllers of their statutory obligations under the DPA. This is a mandatory role and has specific tasks and requirements, outlined in the DPA. The DPO will promote this policy, monitor compliance and provide advice to departments regarding the correct processing of personal data and data protection related issues.

Heads of Departments (for HQ) and Station Managers (for Stations) are accountable for compliance with Data Protection requirements within their area, and must ensure that employees are adequately trained and competent prior to

handling or using personal data. Detailed management actions can be found in Section 6.

All employees must comply with the requirements of the DPA, and supporting and related information policies and procedures.

DETAILED PROCEDURES

4. The Legislation

On 25th May 2018, the Data Protection Act 2018 became the UK's third generation of data protection law, which has modernised the law to ensure it is effective in years to come. It builds on the 1998 legislation and transposes the Law Enforcement Directive into UK law.

'Law enforcement' processing is: the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This processing is likely to apply to Protection services.

The UK General Data Protection Regulation (GDPR) encompasses 'general' processing, which covers everything outside of the scope of 'law enforcement' processing. Examples include training, human resources, health, payroll, and Prevention services.

5. Registration and Fee

The Data Protection Officer (DPO) is responsible for maintaining registration with the Information Commissioners Office (ICO) and paying an annual fee on behalf of the Service. Failure to pay the Information Commissioner promptly can incur financial penalties. The DPO is the primary point of contact for the ICO.

Managers must advise the DPO promptly of any significant changes to personal data processing within their area during the year to enable the DPO to maintain appropriate records which demonstrate compliance with the DPA.

A copy of the registration can be obtained from the Information Commissioner's website at www.ico.gov.uk

6. Management Actions

Departmental Heads and managers must ensure that any personal data processing within their remit, (including by any third parties who process data on behalf of the Service), complies with the DPA principles *(see Appendix 2)* and requirements.

This requires provision of appropriate training, monitoring compliance with information policies and procedures, and implementation of local procedures that protect data and comply with the DPA principles.

In particular, management must ensure procedures support compliance with the principles individuals' rights, safeguards special category data, minimises personal data, and promotes privacy by design and default through Data Protection Impact Assessments *(see Appendix 2)*.

Refer to the Appendix section for details and contact the Information Compliance team for support if required.

7. Privacy Statements (Fair Processing Notices)

Managers of departments or teams who collect or handle personal data must ensure that individuals' are advised how and why their personal data is processed. This must generally be by provision of a leaflet and published on the website. There are limited circumstances where privacy notice does not need to be provided – refer to the ICO website for details.

Privacy statements help to ensure that personal data processing is "fair" and '"transparent" under principle one of the DPA. The Privacy notice must be written in plain English and appropriate for the audience.

If the data is sensitive, or the use of the data is less obvious the Privacy Notice should be more comprehensive and informative.

High level privacy statements are published on the Service website. Managers must ensure copies are available on request, that staff are familiar with the contents of the privacy notice, and provide more specific privacy notices for processing where:

- children or at risk adults are involved,
- where the data processing is complex or unusual,
- where the data processing requires consent.

Children: Where services are offered directly to a child, the privacy notice must be written in a clear, plain way that a child will understand.

The contents of the privacy notice are defined by the DPA *(see Appendix 4 for requirements)*.

8. Information Sharing

Information sharing must adhere to data protection and security standards, and only the minimum amount of information required to achieve that purpose must be shared. Logs of data disclosed must be documented (who disclosed, when, why and to whom). These must enable the Service to meet Subject rights (e.g. rectify or prevent processing) and provide for monitoring and audit.

Personal data can only be transferred outside the European Union if appropriate safeguards are in place or the country has been deemed as offering an adequate level of protection. This means use of Cloud services may not be appropriate. Contact Information Security for advice.

Where required, HoDs will ensure agreements or contracts are in place with any third party agency, joint controller, or data processor. Information sharing agreements will comply with the data sharing policy and ICO code of practice on information sharing.

9 Individuals rights and subject access

Individuals have specific rights over their personal data by applying either in writing or verbally and must be given a response within one month. These rights are:

- the right to be informed about the processing of their information;
- the right of access to their information and to be given a copy;
- the right to rectification, erasure and to restrict processing of their information;
- rights to be told about and object to automated decision-making and profiling.
- the right to data portability (applies to 'general' processing only); and
- the right to object (applies to 'general' processing only).

Individuals also have the right to complain to the Information Commissioners Office if their rights are not upheld and may be able to claim compensation for distress caused by breach of the DPA.

Departments may provide access to personal data within existing processes, for example within Fire reports, or access to employee personal files. These processes must comply with DPA subject access requirements (ie provide a written response, securely, within one month) but will usually be handled by the Department with support from the Information Compliance team if required.

Where individuals submit a formal subject access request, either relating to specific information, or requiring a full search for information Department Managers should contact Information Compliance for guidance.

See Appendix 3 for more information.

10. Breach reporting

All staff must report personal data breaches in accordance with the security incident management and reporting policy. A personal data breach (also known as a security breach) means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach is more than just about losing personal data.

Employees who breach the DPA and commit an offence will be investigated, and may be subject to disciplinary proceedings.

11. Third party contractors/agencies

The Service remains responsible for Service data shared with or processed by third parties, suppliers or other agencies on behalf of the Service.

The Head of Department or Information Owner will ensure that agreements and contracts setting out appropriate DPA requirements (and individuals' access rights) are in place with any third party/agency used to access or handle any personal data on behalf of the Service.

The agreement or contract must usually include the right to audit.

12. Complaints

The Information Commissioner is ultimately responsible for monitoring, investigating and enforcing the Data Protection legislation.

The Information Commissioner requires that complaints are first brought to the attention of the Service, to provide an opportunity for investigation and solution. Any complaints should be directed to the Data Protection Officer, who will review the circumstances of the complaint in consultation with the Department Head.

If the complainant is still not satisfied, they can then complain to the Information Commissioner. The maximum financial penalty for breaching the DPA is €20 million.

APPENDIX

Appendix 1. Definitions

The term “personal data” has a broad meaning and means data relating to a living individual, who can be identified from the data or other available data. Personal data includes facts, opinions or intentions relating to the individual.

Personal data tends to be biographical, affect the person’s privacy, or be primarily about the individual. Examples include:

- name,
- address,
- date of birth,
- CCTV
- IP addresses
- location
- other factors specific to a person such as social identity, physical characteristics etc

Special Category Data is personal data which requires more protection and should only be collected and used where it is justified. Examples include:

- racial or ethnic origin,
- political opinion,
- religious or philosophical beliefs,
- trade union membership,
- genetic or biometric data,
- health and a person’s sex life or sexual orientation.

The Service collects personal data within a wide range of processes, for example:

- HR and personnel records
- Service Directory and contact details;
- Duty Rota Information;
- Incident and mobilising data concerning callers/casualties/public;
- Community safety data which identifies residents or other individuals
- Investigations and offences

This list is not exclusive.

Appendix 2. Data Protection Principles and Department Procedures

Department managers and information owners must identify any personal data handling and implement and monitor appropriate data handling procedures which ensure that employees comply with the six principles (see list below), and individual's data rights.

Data Protection Principles

Data must be:

1. processed lawfully, fairly and for 'general' processing, in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary for that purpose (not excessive).
4. accurate and where necessary, kept up to date;
5. kept for no longer than is necessary for that purpose or purposes; and
6. processed in a manner that ensures appropriate security, using appropriate technical or organisational measures to protect against unauthorised processing, accidental loss, destruction or damage

The Service must also be able to demonstrate compliance with the principles. Heads of Department (HoD) will ensure their area of business implements and monitors appropriate polices and procedures which outline compliance with the principles, individual's rights and how the organisation safeguards special category data.

Conditions (lawful basis) for processing:

All personal data processing must identify one of the six conditions for processing.

These are:-

1. Consent: the individual has given clear consent, informed and unambiguous consent for you to process their personal data for a specific purpose.

2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

4. Vital interests: the processing is **necessary** to protect someone's life.

5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (*This condition cannot be applied if the Service is processing data to perform official tasks).*

Conditions (lawful basis) for Special Category data

Processing this type of data requires an additional condition for processing.

These are;

1. Explicit consent: the individual has given clear consent, informed and unambiguous consent for you to process their personal data for a specific purpose.

2. Employment, security or social protection law: the processing is necessary for these purposes and is authorised by law.

3. Vital interests: the processing is **necessary** to protect someone's life.

4. Not-for-profit organisation: The processing is carried out in the course of it's 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.

5. Manifestly made public: personal data has been made public by the data subject.

6. Legal claims: the processing is necessary for the establishment, exercise or defense of legal claims.

7. Substantial public interest: the processing is necessary for reasons of substantial public interest and has a clear basis in law.

8. Occupational medicine: the processing is necessary for the purposes of occupational medicine for the assessment of the working capacity of the employee and medical diagnosis etc.

9. Public health: the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-boarder threats to health.

10. Archiving the processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.

Detailed guidance on identifying appropriate conditions is available on the ICO website at www.ico.org.uk

Children

Children under the age of 13 cannot give consent themselves; instead consent is required from a person holding 'parental responsibility'. This does not apply where the processing is related to preventative or counselling services offered directly to a child.

Privacy by Design and Default

The Service will implement technical and organisational measures to promote, consider and integrate data protection and privacy into data processing activities from the start of a project or initiative, and maintain good data protection throughout its lifecycle.

This includes ensuring Data Protection Impact Assessments (DPIAs) are conducted where required (see DPIA guidance), implementing risk-based security measures (including encryption), and adopting data protection compliant policies.

Appendix 3. Formal Subject Access Request process

Requests should be logged on the information register held by the PA's team for monitoring purposes.

If the request is unclear, seek clarification from the individual. Until clarification is received, the 1 month deadline is suspended.
Responses should be sent directly to the requester and not via the FOI support email for privacy reasons.

Managers must keep a copy or other suitable evidence of the items released, for 2 years in case of query or complaint, and inform the FOI support team of the date that the response was issued.

Exemptions for requests

There are some exemptions which may apply to requests if a response could prejudice:–

- negotiations with the requester;
- management forecasts;

- confidential references given by us or provided to us
- information used for research, historical or statistical purposes;
- information covered by legal professional privilege.
- crime prevention and detection
- Third party information where disclosure would breach their rights and confidentiality.

If any of these may apply contact the Information Compliance team or Legal Team for further support.

Check identity

Obtain proof of identity such as a driving licence or passport before supplying any personal data to avoid identity fraud, unless you know the person concerned.

Note that an email address is not evidence of identity, as an email account can be set up in any name.

"All the information about me"
If an employee asks for "all the information about me", then managers should write and explain that we will provide a copy of the information contained within their

- personal file,
- training records,
- medical reports and
- appraisals,

If they require any other specific information they should let us know. This will reduce costs to the public and ensure that the correct information is provided.

In any case managers must take all "reasonable steps" to locate the personal data. information which they want copying.

Employee personal data may also be held in:-

- Personal Record file (PRF)
- Any local manager files/folders including development, absence management, training, 1:1's etc
- Emails directly relating to the employee
- Appraisals and performance files/folders
- Disciplinary/grievance files, (consider if there is relevant information within other employees file)
- Minutes of meetings about the employee
- Exit interviews, (including those from other staff who may have had contact with the requestor)
- Any feedback about the employee from other people

- Contact previous line managers to establish and locate other sources of information

This is not an exhaustive list.

Searches may also have to be made of all relevant email accounts, system drives, databases and manual systems. You should confirm that no information is held on individual PC's. The individual's name, or other identifier (such as employee number) can be used to search titles of folders and documents, or the subject line of emails.

Review data located to ensure that the data relates to the person who made the request, and not another individual with a similar name.

Check that any third party data within the response does not breach the DPA – refer to third party section below.

Search for data requested by members of the public in:-

- Operational Policy and assurance
- Service Delivery
- Prevention and Protection
- Democratic Services (complaints and investigations)

Requests on behalf of an individual

An individual can make a request through an agent such as a solicitor or adviser, provided they or their agent provide evidence such as an authorisation letter that they are acting on behalf of the data subject before any personal information is disclosed. This is to prevent unauthorised disclosure and breach of privacy.

Third party data

A request for the personal data of another individual may breach the rights of the person who the data is about and must generally be anonymised unless -

- The data is already known or in the public domain
- The individual who the data is about has given consent to release
- The individual who the data is about has no expectation of confidentiality
- The data release will not cause distress to the person who the data refers to
- The information is purely business/work related about a person working in a professional capacity (this excludes employees working at a junior grade)

Any data released to a third party must be noted in the departmental disclosure log because the individual may ask who has seen their data and we must have a clear audit trail.

Personal data security

Appropriate security must be used when providing personal data. Use secure email if possible or you may need to ask the individual to collect the data and provide evidence of identity.

Data amendments

Data must not be amended or deleted after it has been requested, even if there are concerns or issues with the data content. The individual is entitled to a copy of the data as it exists at the time. The only exception to this rule is to allow normal scheduled amendments to be made.

Excess work

In some limited situations there may be some discretion when answering repeated or unreasonable requests. Contact the Information Compliance team for advice.

Appendix 4. Privacy statement requirements

What information do you need to provide?	Collected from individuals	Obtained from other sources
The name and contact details of organisation	✓	✓
The name and contact details of representative	✓	✓
Contact details of the data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third country or international organisation	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓