# Data Protection Safeguards Policy

## The Processing of Special Category Data

The Data Protection Act 2018 (DPA) sets out an obligation on Cheshire Fire and Rescue Service to have an appropriate policy document in place when relying on certain conditions to process sensitive, special category and some criminal offence data. This policy documents the safeguards required to comply with Part 4 of Schedule 1, DPA (for general processing) and Section 42, DPA (for law enforcement processing).

## 1. About special and sensitive data

Special category and sensitive data is defined as;

- The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
- The processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual,
- The processing of data concerning health,
- The processing of data concerning an individual's sex life or sexual orientation

The Service is a competent authority for the purpose of Part 3 of the DPA. This means we process some personal data when we exercise our law enforcement powers in respect of commercial premises under The Regulatory Reform (Fire Safety) Order 2005. However, it is unlikely that we will process sensitive data for this purpose.

We do, however, process special category data under the GDPR and Part 2, Chapter 2 of the DPA 2018. This is commonly referred to as 'general' processing.

We also process criminal offence data under Part 3 of the DPA and the GDPR. Although this is not defined as special category data, the GDPR requires us to have an appropriate policy in place for its use.

Please visit our privacy notice pages at www.cheshirefire.gov.uk for further information on how we use special category data which do not require an appropriate policy document, such as when we rely on explicit consent.

## 2. Using special category data

We only process special category data for general processing to the extent that it meets a lawful basis from Articles 6 and 9 of the GDPR and where required, a condition listed within Schedule 1 of the DPA. We only process criminal offence data for general processing to the extent that it meets a lawful basis from Articles 6 and a condition listed within Schedule 1, of the DPA.

We describe the relevant Schedule 1 conditions we rely on below which are required by this policy, along with a description of the special category and/or criminal offence data used.

## Employment, Social Security and Social Protection

Physical, mental health and/or disability data may be processed for the purposes of workforce planning, fitness testing, and trauma risk management. It may also necessary for pension/payroll and employee relations purposes such as ill-health retirement, attendance cases and the occupational health process. Trade Union membership details may be processed for the purposes of salary deductions.

## Statutory etc. Purposes

The nature of injuries may be processed for the purposes of accident reporting in accordance with the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) and Health and Safety at Work etc. Act 1974.

Physical, mental health and/or disability data may be processed within personal risk assessments under the Health and Safety at Work etc. Act 1974 and the Management of Health and Safety at Work Regulations 1999. It may also be processed for industrial relations purposes, along with trade union membership, in accordance with Trade Union and Labour Relations (Consolidation) Act 1992 and The Transfer of Undertakings (Protection of Employment) Regulations 2006.

We also conduct driving license checks of individuals who use Service-owned vehicles in compliance with the Road Traffic Act 1988. This may reveal speeding offences. We also need to ask an individuals' ethnic origin as part of the recruitment process in order to check their eligibility to work in UK under Asylum & Immigration Act 1996.

HMICFRS Inspectors could also require us to provide any of the special categories of personal data that it holds in order to provide them with the necessary information about the Service that they require.

## Equality of Opportunity or Treatment and Racial and Ethnic Diversity at Senior Levels of Organisations

Physical, mental health and/or disability data, together with race, ethnic origin, political/religious beliefs, and sex life/orientation may be collected by us for equality monitoring purposes. We also keep records of racial and ethnic diversity at senior levels of the organisation. We strive to collect this type of information anonymously. Some criminal offences may also be processed in accordance with this condition and the Rehabilitation of Offenders Act 1974.

## Preventing or Detecting Unlawful Acts

We may collect criminal offence data of prospective employees and volunteers during the recruitment process. We may also process information relating to actual or alleged offences, where necessary, within our youth engagement programmes for safeguarding purposes. This could also include some detail about an individual’s sex life.

We may use information about crime at an address if it is known to us, such as domestic violence or an arson threat, to provide essential information to crews in emergency response situations. This is necessary to protect our staff and others.

## Protecting the public against dishonesty

We may use criminal offence data during recruitment and within employee relations to protect the public against dishonesty, malpractice, seriously improper conduct etc.

**Safeguarding children and individuals at risk**

Some detail about sex life, ethnicity, physical, mental health and/or disability may be processed within our youth engagement programmes if necessary for safeguarding.

**Insurance**

The nature of injuries are processed for the purposes of accident and event reporting and insurance. We may also need to be advised of employee speeding offences in order to comply with the requirements of insurance policy where they drive Service-owned vehicles.

# 3. Compling with Data Protection

We have a number of measures in place which help to demonstrate compliance with the DPA and its Principles. For example, we have an appointed Data Protection Officer, maintain documentation of our processing activities, have mandatory training, audit, monitoring, appropriate information assurance policies, contractual agreements and information sharing agreements in place. We also carry out Data Protection Impact Assessments (DPIAs) where required.

A description of the DPA principles, along with a summary of our procedures for complying with these principles, is outlined below.

**The first principle** - 'lawful, fair, and transparent'

All processing of personal data, including special and criminal data is documented and included within our Records of Processing Activity (RoPA). The processing is lawful and fair as we have identified an appropriate lawful basis from Article 6 of the GDPR (and Article 9 for special category data). Where required, we have also identified a condition listed within Schedule 1 of the DPA.

We are open and honest when we collect special category and criminal data. We ensure we do not mislead or deceive people by making privacy information available on our website and to individuals direct where relevant.

**The second principle** – 'purpose limitation'

We are authorised within the Service to process personal data for a number of specified purposes. These are identified within our RoPA. We only re-use data if further use is compatible with the original purpose collected or it is authorised by law. We make every effort to inform you of any re-use where it is possible to do so. This tends to be through our privacy notices or through direct contact with our staff.

If we plan to use personal data for a new purpose (other than a legal obligation or a function set out in law), we check that it is compatible with our original purpose. We achieve this through completion of mandatory DPIAs, the data sharing procedure, mandatory data protection training and adhering to departmental procedures.

**The third principle** - 'adequate, relevant and not excessive'

We will only process special category data where it is necessary and proportionate to our stated purpose(s) for processing. We achieve this by conducting mandatory DPIAs, data protection training and ensure appropriate access level controls are in place. Where sensitive personal data is provided to us or obtained by us but is not relevant to our stated purposes, we will erase it.

**The fourth principle** – 'accurate and up to date'

Where we become aware of any personal data which is inaccurate or out of date, we will take every reasonable step to ensure it is erased or rectified without delay. Where we decide not to erase or rectify, we will document our decision.

We also take reasonable steps to verify data before we send it externally. If it becomes apparent that inaccurate data has been shared, we will inform the recipient as soon as possible.

**The fifth principle** – 'kept for no longer than necessary'

We have a corporate retention policy which outlines the minimum retention requirements for the records held by the Service. We also provide an indication of the relevant retention period(s) within our suite of privacy notices held at www.cheshirefire.gov.uk.

**The sixth principle** – 'appropriate security'

We have a number of information assurance policies which provide a framework for ensuring personal data is adequately protected. Our electronic systems and physical storage have appropriate security and access controls applied. We also have a process and procedure for recording and, where necessary, reporting any personal data breaches to the Information Commissioner's Office.

## 4. The Information Commissioner's Office

Regulation of the DPA is the function of the Information Commissioner's Office (ICO). We will fully co-operate with the ICO and will make any relevant data required to perform its tasks, including this policy, available to them without charge.

This policy satisfies the requirements of Part 4 of Schedule 1, DPA. It is therefore an appropriate policy document in support of our compliance with the first data protection principle.

This policy will be reviewed annually or revised more frequently if necessary by the Data Protection Officer or Information Compliance.

Last updated: April 2020