

FAIR PROCESSING AND PRIVACY NOTICE

Employee

Introduction

This data protection Fair Processing and Privacy Notice relates to the personal information that Leicestershire Fire and Rescue Service (LFRS) processes about you as your employer. Processing means the collection, recording, storage, use, sharing, archiving and deletion of your personal information.

This is to help you understand why we need to obtain, hold and use personal information about you during recruitment and selection, throughout your employment and for a period of time after your employment has ceased. It also explains how its use is compliant with current data protection legislation.

Data Controller

A Data Controller is the organisation that decides why and how personal data (personal information) is processed. It is a Data Controller's duty to enforce data protection guidelines. In compliance with the UK General Data Protection Regulations (UK GDPR) tailored by the Data Protection Act 2018, LFRS is the Data Controller for your personal data and special category personal data.

We recognise the importance of protecting personal and confidential information in all that we do and take care to meet our legal, moral and ethical duties. We put in place all reasonable technical, security and procedural controls required to protect your personal data for the whole of its life cycle. Our Personal Data Policy outlines what we aim to do, our personal data Service Procedures and guidance detail how our staff can support compliance with the policy aims.

Reasons why we collect and process your personal data

- Recruitment and selection;
- Contract of employment and onboarding;
- The administration of your salary, wage, pension, sickness, maternity, travel / subsistence payments and any other monies;
- Your health and well-being;
- Your safety;
- Security including personal identification;
- Your training and development requirements;
- Employee relations. Such as human resource planning, conduct, Equality Diversity and Inclusion (EDI), employee consultation, personal appraisals, disciplinary and grievance issues;

- The assessment and arrangement of insurance cover where this is required, such as for car leasing purposes;
- The operational, day to day management and administration of employees by line managers;
- To ensure that we can maintain our Operational Response capability in meeting our purpose of 'Safer People, Safer Places';
- To ensure sufficient resources with the required skills are available to perform the functions and tasks as published in the Fire and Rescue Services Act 2004;
- To ensure sufficient resources with the required skills are available to meet our responsibilities as published in other legislation relevant to the Fire and Rescue Service and the role we play in working with our partners and delivering services to our communities;
- For access control to our premises, car parks and other automated equipment/systems.

We keep and use this information to manage our relationship with you fairly, lawfully and transparently.

The personal data we collect and process

Includes:

- Identifiers such as your name, address, date of birth, Service/employee number and national insurance number;
- Your contact information including telephone numbers, living address(s), email address(s); and that of others you share with us (such as your next of kin, beneficiaries and Doctor);
- Employment and qualification details;
- Disclosure and Barring Service (DBS) check results;
- Salary and wages information including your bank details for payment;
- Membership of representative body (subscription);
- Tax and pension details;
- Contractual details relating to terms and conditions of service;
- Equality, Diversity and Inclusion (EDI) information for monitoring purposes;
- Disability;
- Sickness and absence detail;
- Health and well-being information;
- Covid pandemic isolation status;
- Covid pandemic individual vaccination status records;
- Measurements (for uniform and personal protective equipment);
- Height/weight/Blood pressure/Vision test results/Lung function test results/Drugs test results/Audiometry test results (medical);
- Moving images (Video and audio) and photographic images;

- Driving license status;
- Vehicle registration number;
- Location/Journeys made (Fleet Management System);
- Opinions and decisions about you;

Our lawful basis for processing your personal data

LFRS has due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and any subsequent data protection legislation and codes of best practice.

The lawful basis for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the Service is processing your personal data:

Consent: you have given consent to the processing of your personal data for one or more specific purposes;

Contract: processing is necessary for the performance of a contract to which you are party to or in order to take steps at your request prior to entering into a contract. An example of this is your contract of employment;

Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations). This includes our legal obligations under the Health & Safety at Work Act 1974;

Vital interests: processing is necessary in order to protect your vital interests or of another natural person;

Public task: the processing is necessary for us to perform a task in the public interest or for our official functions as a Fire and Rescue Service, and the task or function has a clear basis in law. Some of the tasks performed by the Service are published in the Fire and Rescue Services Act 2004;

Legitimate interests: the processing is necessary for our 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.

We also process your special category personal data (also known as sensitive personal data), this relates to your:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data and biometric data processed for the purpose of uniquely identifying you;
- Data concerning your health and wellbeing; and
- Data concerning your sexual orientation.

The lawful basis for processing your sensitive personal data is set out in Article 9 of the UK GDPR. In addition to one of the conditions set out in Article 6, at least

one of these must also apply whenever the Service is processing your sensitive personal data:

Consent: you have given explicit consent to the processing of your sensitive personal data for one or more specified purposes;

Our rights as an employer in the field of employment: processing is necessary for the purposes of us carrying out our obligations and exercising our specific rights as the personal Data Controller in the field of employment and social security and social protection law;

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

Legitimate interests: 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 you and that your personal data is not disclosed outside that body without your consent;

Information you have made public: processing relates to personal data which has been manifestly made public by you;

Defense of legal claims: processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity. This includes that relating to information, people, property and vehicles;

Substantial public interest: processing is necessary for reasons of substantial public interest;

Processing by a Health Professional: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

Public Health: 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;

Research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR Article 89.

How long we keep your personal data for

The period that your information is retained for varies according to statutory requirements and other legitimate business reasons. We have set out these retention periods within our Corporate Register Of Processing Activities (ROPA).

The ROPA also details what lawful processing condition we are applying in processing your personal data.

This register is published on our Intranet on Sharepoint and outside of this can be made available on request.

How we keep your personal data safe

We carry out Data Protection Impact Assessment's (DPIA's) to identify our privacy risks and consider 'privacy by design' features in our information systems and our processes. Our information systems are secured using multiple security levels including passwords and can only be accessed by those who have been authorised by us to use them.

All of our staff receive initial mandatory data protection training which is refreshed every two years.

We have robust Policies, Service Procedures and guidance in place to support the technical measures we apply to help safeguard your personal data.

Who we share your personal data with and why

Your privacy is protected by law, which says that we can share your personal data only if we have your consent (permission) or other lawful reason to do so including legal exemption. The reasons why we may disclose your personal data to others (third parties) are:

- To provide contact details internally within the Service, to other local public sector organisations such as local authorities, health trusts, other Fire and Rescue Services or business partners where this is relevant and appropriate to your role and position via public directories containing information about services we provide;
- To other staff in connection with your employment;
- Other parties processing your personal data on our behalf that administer salaries, pension, payroll and other monies and for accounting/budgeting purposes – we term these Data Processors;
- To our Occupational Health Unit for wellbeing and health monitoring and treatment Services provided by them such as physiotherapy or counselling.

We will only make other non-routine disclosures:

- By law, when we are obliged to provide the information requested. For example, to the Inland Revenue or Asylum and Immigration Office;
- By law, to support national fraud initiatives (NFI). For example, to the Audit Commission - this may involve your information being used in data matching exercises, we will advise you when such exercises are to take place;
- To prevent and detect fraud/crime – we are under a duty to protect the public funds we administer and may use information you have provided for this purpose. We may also share information with other bodies administering or in receipt of public funds solely for this purpose;

- For the assessment or collection of any tax or duty when we need to take legal advice for prospective legal proceedings. For example, to our insurers because of a claim being made by you or a customer/client with whom you have been involved as an employee;
- In the course of disciplinary, grievance or other investigations of a similar nature;
- To recover any monies you may owe the Service. Note that we have an expectation that as an employee you will not incur debts on the Service;
- If you have given your consent.

We will never share or sell your personal data to external companies for marketing purposes.

Your rights

Under data protection legislation, you have individual rights in relation to your personal data. It should be noted that they are not absolute rights and are subject to consideration before we act on them. Your rights are:

- To ask us what personal data we hold about you;
- To request to see or have a copy of personal data relating to you. Note: This is called a Subject Access Request (SAR). Such requests should be made in writing to us. Before disclosing information we will need to verify your identity;
- If data we hold is incorrect, you have the right to ask us to update it. If we disagree about it being incorrect we will record the fact that we disagree and may not change it.

Where there is a dispute in relation to the accuracy or processing of your personal data, you have the right to request a restriction is placed on further processing until the dispute is resolved;

- To request that we restrict how we process your personal data;
- To object to us using your personal data and ask us to stop processing it;
- To have it permanently and securely deleted (where there isn't a legal requirement or valid business reason for us retain it). This is sometimes called the right to erasure;
- To ask that we transfer it into a portable format (in certain circumstances);
- Where we process your personal data based on your consent, you have the right to withdraw that consent at any time.
- The right to lodge a complaint with the Information Commissioners Office (ICO) if you are not satisfied with how we are processing your personal data.

Contacts - Data Protection information, requests and complaints

If you would like to exercise your individual rights or discuss anything in this Privacy Notice, please contact:

Data Protection Officer (DPO): Information Governance Manager (DPO)

In writing address: Leicestershire Fire and Rescue Service, 12,
Geoff Monk Way, Birstall, Leicester, LE4 3BU

Telephone (switchboard): 0116 210 5555

Email: dpo@leics-fire.gov.uk

If you have concerns about the use of your personal data, the Information Commissioners Office is an independent body set up to uphold information rights in the UK. They can be contacted through their website: www.ico.org.uk or their helpline on 0303 123 1113, or in writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

For more information about your rights:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

To complain to the Information Commissioner's Office:

<https://ico.org.uk/concerns/>

Before lodging a complaint with the Information Commissioners Office, you are encouraged to contact our Data Protection Officer to see if the matter can be resolved by us.

Review

First published May 2018.

Revised June 2019.

Revised July 2021.

Next review July 2022.