LONDON FIRE BRIGADE

Data protection and privacy policy

New policy number:	**351**
Old instruction number:	
Issue date:	**20 April 2004**
Reviewed as current:	**6 October 2025**
Owner:	**Chief Information Officer**
Responsible work team:	**Information Governance Team**

Contents

1 Introduction

1.1 This policy outlines the London Fire Brigade's procedures in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data it holds about a living individual. The LFB's Head of Information Governance has delegated responsibility for data protection and is the Data Protection Officer for the Brigade. The Information Access Team within Information Management provide day-to-day help, support and guidance for managers and staff and they can be contacted for help and advice.

1.2 Personal data is any information (including opinions and intentions) which relates to an identified or identifiable person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data.

1.3 The Information Commissioner (ICO) is the UKs data protection supervisory authority and they maintain an extensive set of guidance and best practice for data protection. This policy is not intended to replace or supersede the Information Commissioners advice, but serves as a working framework in which LFB staff can operate day to day. As such, the advice and policy statements in this policy should be followed by all employees, agency staff and contractors who process or have access to personal data held by the Brigade.

1.4 Any matters that extend beyond the remit of this policy or over which there is dispute or uncertainty must be referred to the DPO and/or the LFB's Information Access Team (dataprotectionofficer@london-fire.gov.uk or informationaccess@london-fire.gov.uk)

2 LFC as a data controller

2.1 Organisations that process personal data are known in data protection law as "data controllers". The London Fire Commissioner (LFC) is the head of the London Fire Brigade and is the Fire and Rescue Authority for London. The LFC is a data controller for personal data and has notified the Information Commissioner (the UK regulator for data protection) of this. The registered address of the LFC is:

London Fire Commissioner
169 Union Street
London SE1 0LL

Registration number is Z7122455.

The Data Protection Officer

2.2 As a public authority, the LFB is required to appoint a Data Protection Officer (DPO). The DPO for the LFB is the **Head of Information Governance**.

2.3 The principal tasks of the DPO as described in data protection law are:

- To provide advice to the organisation and its employees on compliance obligations.
- To advise on when data protection impact assessments are required and to monitor their performance.
- To monitor compliance with the data protection law and organisational policies, including staff awareness and provisions for training.
- To co-operate with, and be the first point of contact for the Information Commissioner.
- To be the first point of contact within the organisation(s) for all data protection matters.
- To be available to be contacted directly by data subjects – the contact details of the data protection officer are published in the organisation's privacy notices.
- To take into account information risk when performing the above.

2.4 For the DPO to fulfil their role it is necessary that:

- The DPO can report directly to the highest management level of the organisation.
- Staff and managers within the organisation involve the DPO in all data protection issues in a timely manner.
- The Data Protection Officer is not pressurised by the organisation as to how to perform their tasks, and is protected from disciplinary action when carrying out those tasks.
- Where the Data Protection Officer performs another role or roles, that there is no conflict of interest.

2.5 The DPO can be contacted by:

Email: dataprotectionofficer@london-fire.gov.uk
Telephone: 020 8555 1200 and ask to talk to a member of the Information Access Team
Write to: Data Protection Officer, London Fire Brigade, 169 Union Street, London SE1 0LL

Data protection within the LFB

2.6 All staff are responsible for ensuring that the LFB comply with data protection law and that personal data is processed lawfully, **fairly, transparently and securely**. The Information Access team can be contacted for help and advice about data protection compliance and **must** be contacted if you become aware of a personal data breach within the LFB.

2.7 The foundation of data protection law and the root of good data protection compliance are the data protection Principles. In broad terms, the principles require that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency'**);
- Collected only for a specified, explicit and legitimate purpose(s) ('**purpose limitation**');
- Adequate, relevant and limited to what is necessary ('**data minimisation**');
- Accurate and kept up to date ('**accuracy**');
- Kept for no longer than is necessary ('**storage limitation**');
- Processed in a manner that ensures appropriate security ('**integrity and confidentiality**').

2.8 In addition there is a requirement that when an organisation process personal data that the organisation:

- Is responsible for, and be able to demonstrate, compliance with the principles ('**accountability**').

Processing personal data

2.9 If you have information that relates to a living individual it is likely that you are processing personal data. Two key definitions within data protection law are the definitions for what is personal data and when it is processed (UK GDPR Article 4).

2.10 **'Personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.11 '**Processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

2.12 The table below describes the categories of personal data processed by the Brigade along with examples of data types. If you are using any of the data types listed in your work, then you will be processing personal data.

Category	**Example of data included in the category**
Personal details	Titles, names, previous names, nick-names, aliases, address, postcode, telephone numbers, email addresses, social media user names, personal websites addresses, signature, emergency contacts, family history, marital status, dependants, next of kin, language skills.
Personal features	Age, date of birth, gender, height, weight, body measurements, eye/hair/skin colour, identifying marks, images - photo/video/audio.
ID Numbers	National insurance number, passport number, driving licence number, social security number, national health number. [Note: this category may include facsimile copies of original documents containing the identifier]
Work details	Pay number, job titles, work addresses, employers name, work contact numbers, work email address, call sign, work social media user names, grade, role, rank, start date, end date, camp out base, work history, computer and communications monitoring information, lone-worker location, vehicle number plate, pager number, leave and absence, proof of right to work, building access records.
Financial details	Salary, payroll records, bank details, pension, tax, allowances, state benefits, property ownership, compensation payments.
Education	Qualification, establishment, establishment address.
Narrative data	Biography, CV, situational description, occupational experiences, behavioural characteristics, professional membership, personal references, performance evaluations, discipline or grievances.

2.13 Some types of personal data are considered more sensitive and have greater level of legal protection. These are called "special category data" and processing is prohibited except in a small number of exceptions. Special category data is data revealing:

- Racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs, or trade union membership;
- processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
- data concerning health;
- data concerning a natural person's sex life or sexual orientation;
- [there are also special rules for processing criminal data].

2.14 If you intend to process special category data, or data about criminal convictions, the process must be approved by the DPO before the processing starts.

Processing data about children

2.15 Children (a person under the age of 18) need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved. If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind. Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.

2.16 Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles online. The information provided to children about the processing of their data must be clear so that they are able to understand what will happen to their personal data, and what rights they have.

3 Information that must be provided when personal data is collected

3.1 A key foundation of the data protection law is that data subjects should be aware of the information being collected about them, by who and for what reason. Data subjects have a right to be informed about the data that is collected and processed about them in a concise, transparent, intelligible and easily accessible form, using clear and plain language and there are statutory obligations about what information needs to be provided.

3.2 To make this information easily available, the Brigade has published a "**Privacy Notice**" on its website. This contains information about the LFC as a data controller and explains the main processing activities of the Brigade. The privacy notice can be found at www.london-fire.gov.uk/privacy and is reproduced in this policy as Appendix 3.

3.3 While the privacy notice is publicly available, it is still necessary to inform people about the existence of the notice and where it can be found (and how else the information can be obtained). You must include information about the privacy notice on all documents (including electronic forms and documents) where personal data is collected.

3.4 There are two versions of the standard text that can be used. The full version must be used at the first opportunity that data is collected or in any correspondence sent at the start of a process where data will be collected. The shorter version can be used in subsequent correspondence with a data subject who has already been informed of the longer text. These are approved texts and must not be altered without permission from the DPO.

Privacy statement

The full version (below) must be used on all data collection forms and/or initial correspondence with a data subject.

> **Protecting your personal data and privacy**
>
> The London Fire Brigade is committed to using personal data in a responsible and transparent way. We will ensure that we protect your privacy and comply with data protection law. In most cases we collect, process and store personal information because we have a legal duty to do so (which may be explicit or implied) or because it forms part of a contract with you. We will share personal information with other trusted organisations if they can help to keep you safe, if they process information on our behalf, or if we are required to by law.
>
> **To find out more about data protection and privacy**
>
> We make the detailed information about data protection and privacy available to you through our 'Privacy Notice' which is published in full on our website. The notice has information about your privacy rights, which include how you can access the data we hold, and how, in some situations, you can stop us from processing the data or have it corrected or deleted. If you want to know more about data protection in the LFB or if you would like a full copy of our Privacy Notice you can:
>
> - Visit: www.london-fire.gov.uk/privacy
> - Email: dataprotectionofficer@london-fire.gov.uk
> - Telephone: 020 8555 1200 and ask to talk to our Information Access Team
> - Write to: Data Protection Officer, London Fire Brigade, 169 Union Street, London SE1 0LL

The short version should be used on all subsequent correspondence with a data subject.

> **Protecting your personal data and privacy**
>
> The London Fire Brigade is committed to using personal data in a responsible and transparent way. To find out more visit www.london-fire.gov.uk/privacy.

4 Privacy by design and default

4.1 It is a requirement of the data protection law that data controllers put in place measures to implement the data protection principles and safeguard individual rights. This requirement is often referred to as 'data protection by design and by default'.

4.2 In essence, this means that the data protection principles need to be embedded into all processing activities and business practices, from the design stage right through the lifecycle. This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change made by the Data Protection Law is that it is now a legal requirement.

4.3 Data protection by design is about considering data protection and privacy issues upfront in everything we do. It helps to ensure that data protection principles are complied with and forms part of the focus on accountability. It also means that data protection cannot be an afterthought when changing business practices or something that can be done at a later time. Ensure compliance and protecting privacy must be a high-level consideration and must be embedded into business changes and the data protection requirements must be delivered along with the business outcomes.

Data protection impact assessments

4.4 Data protection impact assessments (DPIA) are a process to help identify and minimise the data protection risks of a project. A DPIA is a requirement when the processing of personal data is likely to result in a high risk to individuals and it is good practice to do a DPIA for any other significant changes which requires the processing of personal data. Within the LFB DPIAs are required for all Corporate Projects and for any significant changes to the way that personal data is collected or processed. The DPO may also require a DPIA in other circumstances to ensure that personal data is being processed correctly. If there is uncertainty about whether or not a DPIA is required, this will be decided by the DPO.

4.5 A good DPIA helps to evidence that you have considered the risks related to your intended processing; and you have met your broader data protection obligations.

4.6 In broad terms a DPIA:

(a) describes the nature, scope, context and purposes of the processing;

(b) assesses necessity, proportionality and compliance measures;

(c) identifies and assesses risks to individuals; and

(d) identifies any additional measures to mitigate those risks.

4.7 If you are collecting new data or making changes to the way that existing data is processed, then you must contact the DPO/Information Access Team to agree whether or not a DPIA is required before you collect new data or make any changes.

5 Data subject rights

5.1 Data subjects – the people we hold information about (including staff, the public, and our partners and stakeholders) – have a number of rights under data protection law. These rights are there so that data subjects can ensure that data controllers are processing their information in accordance with the data protection principles.

5.2 Data subjects have the right to have access the information held about them and to ask data controllers to; rectify or erase data ('right to be forgotten'), restrict the processing of their data, have their data transferred to another provider (portability) and the right to object. Data controllers must respond to such requests and comply unless they have a lawful reason not to.

5.3 Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Right of access (subject access request – SAR)

5.4 A subject access request (SAR) is a request from an individual (data subject) for information about them (personal data) that the LFB holds. Under data protection law, SARs must be replied to within one calendar month (with very few exceptions).

5.5 If you are a member of staff wanting to make a subject access request to the Brigade for your own data, please see section "LFB staff requesting their own personal data".

Right to rectification or erasure

5.6 It is a data protection principle that personal data must be up to date and not held for longer than necessary. That being the case, in many cases it will be appropriate to update information about individuals in line with a requestors wishes. However, whilst the requestor has a right of request, that does not mean that the Brigade has to comply with that request, where there is a compelling and justifiable reason not to. In such cases, the advice the information access team/DPO must be sought so that the circumstances can be fully established and that a formal refusal notice can be issued to the requestor.

Other rights

5.7 If a data subject would like to exercise any of their other data protection rights (e.g. portability, restriction or objection) then you should notify the Information Access Team/DPO at the earliest opportunity so that the request can be considered and processed correctly.

6 Handling subject access requests

Recognising a request

6.1 It is important that staff and managers know how to recognise a SAR when they see one. Any member of staff could receive a SAR. Additionally, it is useful for staff to know that they are entitled to make a SAR and how to do this. A request does not have to include the phrase 'subject access request' or mention GDPR or data protection law, as long as it is clear that the individual is asking for their own personal data.

6.2 Where it is clear that a requestor is formally exercising their right to access their personal data (in the context of data protection law), then these requests should be bought to the attention of the Information Access Team (by email to informationaccess@london-fire.gov.uk or by telephone on 0208 8500 1200) for advice about the best way to proceed.

6.3 A subject access request may be made verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point.

6.4 If someone is making a verbal request to you, you should check with the requester that you have understood their request, as this can help avoid later disputes about how the request has been interpreted. You should advise them to confirm a verbal request in writing (e.g. in an email).

6.5 Where the Brigade processes a large quantity of information concerning a data subject (such as employees), it is usually reasonable to ask that the data subject specify the information or processing activities to which the request relates (for example, focusing on a specific activity or timeframe, or naming the team or people who are likely to hold the information). It is also important to establish whether the information requested falls within the definition of personal data. The ICO has published guidance on what is personal data here.

Openness and transparency

6.6 The Brigade values openness, honesty and transparency and in most cases managers should not be afraid to provide people with the information you might hold about them. In most cases, people are just interested in having a copy of the information you recorded; this might be copies of meeting notes, information contained in a letter or an extract of information held on computer systems. If the information is about them, they know what the information is and why it is held, and you have no business reason not to disclose, you can provide the information.

6.7 Remember, an individual is only entitled to their own personal data, and not to information relating to other people. If the information they want about themselves, includes personal information of others, then you should not provide it unless you remove the other personal information by redaction.

6.8 If the request is not straight forward, or if the information may also contain information about other people, or if there are business reasons to consider not to release the information, then these request must be referred to the Information Access team at the earliest opportunity (the legal requirement to respond within one calendar month starts when the request is received by the Brigade).

7 LFB staff requesting their own personal data

7.1 If you are a member of staff and want to access you own data, or exercise any of your data subject rights, then you should contact the Information Access Team (by email to informationaccess@london-fire.gov.uk or by telephone.

7.2 The team will process your request and respond within the statutory time limit of one calendar month. If you need the information urgently, and can't wait a month, then you will need to discuss this with the team. The Brigade cannot undertake to provide information in a shorter period than one calendar month, but will consider sympathetically any request where there is urgency.

7.3 In requesting information, you should try and be specific about what you want (e.g. emails to/from a particular person, documents between certain dates, or information on a particular topic). We can ask you to focus your request. You should be aware that depending on the information you request; we are likely to have to ask other members of staff to provide the information. If you are not happy about other people being contacted, then you should discuss this with a member of the Information Access Team.

7.4 You are expected to make reasonable requests when asking for your data, particularly if you have been employed with the Brigade for a number of years. You should avoid making unspecified requests such as asking for "all data held about me" or "everything where I am mentioned". If a request appears to lack focus, you may be asked to clarify what activity or process your request relates to. The requirement on the Brigade is to make reasonable and proportionate searches for the information, so the more specific you can be, the more likely the information you are looking for can be located.

7.5 You should remember that a lot of the personal data about you will be held on your electronic personal record file (ePRF). To access your file, go to Hotwire and select HR, pay and employment from the home page, then select Your details, then select Electronic Personal Record File.

7.6 Not everything that mentions you by name will be personal data. The Information Commissioner has published guidance about what is personal data and you can access this on the ICO website here.

7.7 There may be some personal information about you, that the Brigade will not be able to provide. There is some limited provision in data protection law to withhold information. The normal reasons for this will be that the information also contains personal data about other people or identifies them as the source of information (witness statements for example), the information is related to criminal investigations or the information is legally privileged.

7.8 For more information see https://ico.org.uk/your-data-matters/your-right-of-access/

Asking the Brigade to review its response to your information request

7.9 If, when the Brigade responds to your request for information, you are not happy with what has been provided (e.g. you believe there is more information, information has been removed (redacted)), you can ask the Brigade to review its handling of your request. The ICO will normally expect you to have first asked the Brigade to review its handling of your request, if you make a complaint to them.

7.10 If you request a review, you must set out the reasons why you believe your request has not been fully met. These reviews will be undertaken independently by the Brigade Data Protection Officer (or their nominated representative); as the DPO does not normally deal with day-to-day requests. The DPO will aim to respond to your review request within a calendar month.

If you are contacted by the Information Access team to provide personal data about someone else

7.11 When a request is processed by the information access team, they may contact the relevant people and departments who are likely to hold the data so it can be collated, and the request responded to with the one month limit. If, as a member of staff, you receive a request from the Information Access Team then you will need to cooperate with that request and without unnecessary delay. All the information requested by the team must be provided and it is an offence for a person (that can be the Brigade or an individual) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

7.12 The Information Access Team can also use eDiscovery tools to search for electronic information, but this will depend on the information being requested and the search may require a combined method of search for the information that involves people and departments.

7.13 If you have concerns about the information being requested, or you think there are business reasons for the information not to be disclosed (or altered or deleted) then you should discuss these with the Information Access Team. There are very few exemptions from disclosure and the decision to apply those exemptions rests with the Information Access Team. If there is dispute about the decision made, then this can be raised with the DPO. If there is a need to get legal advice on disclosure requests, then the Information Access Team/DPO will initiate this with General Counsel.

7.14 In all cases, you will need to provide all of the relevant information to the information access team, whether or not it is exempted from disclose or not. This is so that there is an accurate record of what information was held at the time of the request and how the exemptions (if any) apply to each individual record, or parts of those records.

7.15 When identifying what information is held by the Brigade this will include all emails, papers, written notes, electronic files and any other recorded information held anywhere by the Brigade. Information about individuals may also be contained in text messages, WhatsApp chat, social media and personal email; if the communication is about work and is work related, it will still fall within the scope of the right of access even if the communication originates on what is otherwise considered to be a private phone, computer, tablet or other device.

8 Data breach reporting

8.1 It is important, and a requirement of the data protection law, that personal data is collected, used, stored and deleted in a secure way.

8.2 A personal data breach means an event that leads 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. It also means that a breach is more than just about losing personal data. For example, personal data breaches can include:

- Access by an unauthorised person;
- Where personal information has been found abandoned/misplaced (e.g. left on a printer);
- Sending personal data to an incorrect recipient;
- Devices containing personal data being lost or stolen;
- Missing or incorrectly filed case notes/personal records;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

8.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

8.4 Appendix 1 "Protecting personal data (Information security)" gives guidance to staff on the types of behaviours and actions that all staff are expected to follow to mitigate the risk of personal data loss.

8.5 The data protection law is clear that when a security incident takes place, that the Brigade must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Actions by LFB staff

8.6 If you become aware of a breach of personal data, or have concerns that a breach will occur, you must inform the Information Access Team and the DPO **as soon** as you become aware of that. It may be that the situation can be resolved quickly and simply, but the Brigade is required to maintain a record of all personal data breaches irrespective of the severity or impact of the event.

8.7 To report a breach, you can email either information.access@london-fire.gov.uk or dataprotectionofficer@london-fire.gov.uk.

8.8 Where you can, try to include these details:

(a) your name and contact details;

(b) the date and time when the breach occurred (or an estimate);

(c) the date and time when it first became known that a breach had occurred;

(d) basic information about how the breach occurred;

(e) information about the type(s) of personal data involved (e.g. addresses, financial data, health records);

(f) an indication of the number of personal data records concerned;

(g) an indication of how many people could be affected.

8.9 Not reporting a known data breach to the DPO can be more serious than being responsible for an accidental data loss and failure to notify the DPO of a data breach is a form of misconduct and may be a discipline matter.

8.10 When a breach, or potential breach, is discovered it will be necessary to investigate those circumstances so that he details and impacts can be established. This investigation needs to happen **in the first 72 hours** of the breach being discovered.

8.11 The investigation will establish:

- The type of personal data involved;
- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The likely consequences of the breach and the possible risks to rights and freedoms of those effected; and
- The measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

8.12 On investigation, the DPO will consider if the individual(s) effected and/or the ICO needs to be informed. If that is the case, the DPO will lead on those actions.

Appendix 1 – Protecting personal data (Information security)

This section of the policy is designed to limit the risk that confidential information is disclosed inappropriately, this particularly applies to personal identifiable data.

Information security ensures the confidentiality, integrity and availability of information is properly preserved and protected. This guidance as part of the Data protection and privacy policy covers security which can be applied through technology and encompasses the behaviour of staff and authorised users who manage the information as part of their work.

Principles

Information security is the responsibility of everyone without exception.

The Brigade has a responsibility to securely manage its information assets, the information about the public, staff, contractors and business partners and to protect that information from unauthorised disclosure, loss of integrity or availability.

Heads of Service are individually responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that their staff (permanent, temporary or contractor), are aware of this information security policy, and user obligations applicable to their area of work.
- Ensuring that their staff are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they are using in their roles.
- Ensuring staff know to contact the Information Access Team about any concerns about information security or to report a data breach.

All employees and staff working for the Brigade are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action.

In particular all staff must understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected breach of information security within the Brigade.

Physical security

Access to buildings must be restricted. Such restrictions include making sure security doors are properly closed and secure cabinets locked. Doors and windows must be secured when the station/building is left unattended. Visitors to non-public areas of Brigade properties are to be accompanied and signed in and out of the premises.

Security of paper records

Staff have a responsibility to keep personal data safe and confidential. Paper records should be stored in secure conditions in a secured area or lockable cabinet, preferably both. Records and papers should not be left on desks in unlocked, unattended rooms or on public view. Care should be taken to prohibit the ability for unauthorised people to access records and papers containing confidential personal data.

Staff should avoid taking records with personal data out of their workplace unless absolutely necessary. Staff who do take records containing personal data from their usual workplace are personally responsible for preserving security of that information.

Mobile workers and home workers

Staff who take personal information away from their work base need to take particular precautions with respect to ensuring confidentiality of this information. The basic principles of confidentiality and data protection must be adhered to – in particular that information must be kept secure.

Where possible you should avoid taking hard copies of documents containing personal identifiable information out of your workplace. Where it is strictly necessary to take physical documents out of the office, you must follow the guidance below.

- Obtain permission from you line manager so that they are aware of, and agree that, the information that is being removed.
- Make a list of the information that is being removed so that if it is lost or stolen it is clear what information is missing and what the risks and impacts may be (see also data breach reporting).
- Use a briefcase or bag that can be securely fastened (for example a bag with a full length zip) to prevent the information from being seen and/or from falling out.
- Travel directly between your workplace and the secondary destination (e.g. office to home; office to external meeting). Do not take the information with you if you are undertaking any personal activities whilst in possession of the information (e.g. do not go to the pub or gym).
- If using a car, the information can be kept locked in the boot when in transit between work, personal activities and the secondary destination.
- When arriving at the secondary destination, check that you are still in possession of all the materials.
- If the documents will be out of sight (e.g. while they are in your home), they should be in a secure place and away from view of other people.
- Do not dispose of any confidential documents until you are back at your workplace.
- Return the document to your workplace at the earliest opportunity and inform you manager of their return.

Transfers of personal information (data sharing)

Regular transfers of personal data should be documented in a Data Sharing Agreement as set out in Policy number 621 – Information sharing arrangements which should specify how the data should be transferred securely. However, all transfer of information carries an element of risk that it may be intercepted by third parties (intentionally or otherwise) or go astray.

Before transferring any personal data three questions need to be considered:

- Is the recipient entitled to this information?
- Is the proposed use of this information clearly identified?
- Is the minimum amount of information necessary being sent?

Only if the answer to all these questions is yes can information be transferred.

This guidance does not encompass the exchange of personal data during live operational incidents during which Incident Commanders will balance the needs to share information with the risk to life involved taking into account the guidance produced by Government in their publication "Data protection and sharing guidance for emergency planners and responders" (https://www.gov.uk/government/publications/data-protection-and-sharing-guidance-for-emergency-planners-and-responders).

All electronic bulk or regular transfers of personal data must be approved and recorded by the DPO.

Conversations

A considerable amount of personal and confidential information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in open plan locations. Care should be taken to ensure that confidentiality is maintained in such discussions.

Where confidential information is transferred by telephone or face to face, care should be taken to ensure that personal details are not overheard by others who do not have a 'need to know'. Such discussions should take place in private locations and not in public areas.

Telephone

If personal and confidential information is to be shared by telephone then steps need to be taken to ensure the recipient is properly identified. Staff must always ensure that they are confident of the identity of a caller and the bona fide nature of their request before imparting any confidential information to them.

Unless staff are certain of the identity of the caller, staff must obtain the caller's name, organisation and main switchboard telephone number (rather than direct dial number). Staff should then end the call and advise that a return call will be placed using the information provided to ensure the identity of the caller. With the information provided by the caller, staff are then able to check, using directories or other sources e.g. yearbooks, that the details provided are correct for the organisation/team identified.

Where practicable, staff should ask for requests about personal and confidential information to be put in writing. Staff must not be persuaded or pressured into giving information just because the caller has a plausible reason for asking for it. Concerns about releasing information in urgent situations should be raised with the Information Access Team.

Computers and email

If accessing Brigade systems from non-secure sites, e.g. internet cafes, hotels, in accordance with Policy number 485 - ICT acceptable use policy, users must ensure they log out and fully close all browsers.

The use of personal portable electronic storage equipment (e.g. USB Memory sticks) is not allowed. LFB encrypted storage devices can be ordered from POMS. Once obtained, the security of the device is the responsibility of the staff member: they must not be left unattended and should be stored securely in a locked area. Any data saved on it for transport must be deleted from the device once moved.

The e-mail transmission of personal and confidential information internally over the Brigade's network poses serious risks to confidentiality. Special care should be taken to ensure the information is sent only to recipients who have a 'need to know': always double check the recipient list to ensure the email is being sent to the correct person.

Use of shared printers

Where staff are linked to more than one printer check they must check documents are being sent to the correct printer. Where secure print functionality (e.g. print cards) is available this must be used. Never send documents to a printer in a common area open to the public or to unauthorised people without using the secure print function.

Good records management

It is essential that staff and managers adopt good records management practices and processes so that personal information can be easily located, within a reasonable time, whilst ensuring that personal information is not kept for longer than necessary and is kept up to date.

For further information on good records management, contact the Records Management Team on extension 30380.

Appendix 2 – LFB's commitment to data protection (the appropriate policy document)

It is a requirement of the Data Protection Law that the Brigade explains how it complies with the data protection principles and that it has a procedure for records management. This is the requirement in the Data Protection Law for an "appropriate policy document" and is required for the processing of special category data and the processing of information about criminal offence.

The statement in this appendix meets the following requirements of the Data Protection Law:

- Paragraph 1 of Schedule 1 requiring that an appropriate policy document be in place where the processing of special category personal information necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.
- Paragraph 5 of Schedule 1 requiring that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest.
- Section 42 requiring that an appropriate policy document is in place in respect of processing of personal information for law enforcement purposes.

Our commitment to compliance with the data protection principles (GDPR Article 5)

The LFC will:

- Ensure that personal data is only processed where a lawful basis applies and where processing is otherwise lawful.
- Only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- Ensure that data subjects receive full privacy information so that any processing of personal data is transparent.
- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we use personal data for a new purpose that is compatible, we will inform the data subject first (unless exempt).
- Only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.
- Ensure that personal data is accurate and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.
- Only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.
- Ensure that there appropriate organisational and technical measures in place to protect personal data.
- Ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request.
- Carry out a Data Protection Impact Assessment for any high risk personal data processing and consult the Information Commissioner if appropriate.
- Appoint a Data Protection Officer to provide independent advice and monitoring of the departments' personal data handling and that this person has access to report to the highest management level of the department.

- Have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

We will ensure, where special category personal data or criminal offences data are processed, that:

- There is a record of that processing and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- Data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- Where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous.
- We retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To work out the right retention period for personal data, we consider the following matters:

- The amount, nature, and sensitivity of the personal data.
- The potential risk of harm from unauthorised use or disclosure of personal data.
- The purposes for which we process your personal data and whether we can achieve those purposes through other means, and
- Any legal or regulatory requirements.

Once services are no longer required from us by a person, we will retain and securely destroy their personal information in accordance with Policy number 879 - Records management strategy 5 – records retention guidance.

Appendix 3 – Advice when working overseas

The UK data protection laws permit processing in the UK, the EU and countries that the EU have awarded adequacy status. Processing personal data in any other jurisdictions is considered to be processing in a 'third country' which requires significantly more security and governance controls to protect the data, (which the LFB does not have in place as it is a UK based organisation).

However, the UK's Information Commissioner has said that they don't consider an employee accessing a remote work server for work purposes to be a transfer/processing" if *you are sending personal data to someone employed by you or by your company or organisation, this is not a restricted transfer*[1]".

In whichever country the data is being accessed, the LFB is still responsible for the security of the data and some countries are at greater risk of crime, and other threats to citizens and tourists than others. It is therefore advised that the following principles are adopted by managers who receive request from staff to work overseas (for any duration).

1. Work should not be permitted in any region of a country where the UK Foreign Office (FCDO) advises against travel or has issued security/safety concerns.
2. The Citrix desktop environment must be used for all work purposes (ie Microsoft 365, or other cloud-based services application should not be directly accessed from outside the Citrix environment). The LFB's Microsoft 365 services have geo-fencing enabled, so access to these services (outside of Citrix) will be automatically restricted for devices in some locations.
3. The device used to access Citrix ("the device") must be an LFB owned and issued device.
4. The device should only be used from a permanent place of residence. It should not be used at coffee shops (or similar) nor transported between multiple locations, other than the return to the UK.
5. The device should be in securable room at the place of residence and the device positioned away from easy viewing by others.
6. No work must be printed.
7. The employee must have completed the online Data Protection and Cyber Security training within the last 12 months.
8. Any data breach or concern about data security must be reported to the LFB as soon as it is discovered.
9. The employee's line manager must assure themselves that the above principles will be adopted.

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/

Appendix 4 – Privacy notice

This appendix reproduces the LFC's privacy notice as it appears on the LFB's public website (www.london-fire.gov.uk/privacy).

Protecting your personal data and privacy

This privacy notice (sometimes called a fair processing notice) explains how the London Fire Brigade ("we" or "us") will use the personal data we hold about you. If we ask you for personal information we will hold a record of why we are asking and why the information is necessary to do our work.

We use the term 'privacy notice' to describe all the privacy information that we make available or provide to people when we collect information about them. Our privacy information is made up of:

- The information we put on the letters, forms and places where data is collected
- The verbal or written information given to you by us when we ask you for your data
- This general privacy notice that explains;
    - why we use personal information,
    - information about us as a Data Controller
    - who the Data Protection Officer is and how to contact them
    - our legal basis for processing your information
    - how we process special categories of personal data
    - consent and when we will ask for this
    - the types of personal data we hold
    - who we share personal information
    - what happens if you don't give us the information we need
    - automated decision making
    - how long we keep personal information
    - your information rights and how to access the data we hold
    - What to do if you have a concern

Why we use personal information

When we collect and process information about you we do so according to UK data protection law. This means we will be fair and transparent about the data we collect and we will keep your information safe. Our main processing activities that use personal data are:

- **Employment** – Employment lifecycle | Complaints, investigations and disciplinary proceedings | Counselling and Trauma | Whistleblowing
- **Emergency incidents and response** – Responding to emergencies and other eventualities | Civil contingencies | National Inter-Agency Liaison | Video recording devices
- **Regulation and protection** – Home fire safety and public wellbeing | Safeguarding adults and children | Fire safety, regulation and enforcement | Law enforcement processing | Data sharing with trusted partners
- **Other services** – Fire Cadets | Firesetters intervention scheme | Museum
- **Cross-functional and business processing activities** – Public sector equality duty | Historical research and archiving | Complaints & compliments | Communications activities, events and media | Security & CCTV | Procurement, supplies and services | Legal

These are described in our Records of Processing Activities which also document which of the UK GDPR lawful bases we are using to process personal data related to these activities. We have also recorded the relevant laws that provide the duties, powers or obligations to collect personal data for those purposes.

LFB as a Data Controller

The London Fire Commissioner (LFC) is the head of the London Fire Brigade and is the Fire and Rescue Authority for London. The LFC is a data controller for personal data and has notified the Information Commissioner (the UK regulator for data protection) of this. Our main address is: **London Fire Brigade, 169 Union Street, London SE1 0LL**. The main contact number is **020 8555 1200.**

Our details have been registered with the Information Commissioners Office (ICO) and our register number is **Z7122455**. The ICO's register can be viewed online at http://ico.org.uk.

The Data Protection Officer

Our Data Protection Officer (DPO) is the LFB Head of Information Governance who has day-to-day responsibility for data protection and information governance issues. The DPO can be contacted via the address or phone number above, or by:

- Email to: dataprotectionofficer@london-fire.gov.uk
- Telephone: 020 8555 1200 ext 30300 and talk to a member of our Information Access Team
- Write to: Data Protection Officer, London Fire Brigade, 169 Union Street, London SE1 0LL

Our legal basis for processing

Our legal basis for processing your personal data will depend on the specific activity we are undertaking. Generally speaking we process personal data for the reasons set out below. In only a very few situations will we ask for your consent for us to use your data as typically we have legal duties or powers then enable us to process personal data to undertake our functions as a fire and rescue service. It will however, often be the case that you will be giving us personal information voluntarily and with your cooperation, but we will process that information on the basis of our duties and powers rather than because you have given your consent.

Our main processing conditions can be described as:

- **Contractual** – we need the information for the performance of a contract we have with you or that you are preparing to enter into with us.
- **Legal obligation** – it is necessary to use the information for compliance with a legal obligation that we must comply with.
- **Vital interests** – we are gathering information as part of an operational incident where there is a risk to someone's life.
- **Public task** – the information is necessary for us to carried out a task in the public interest or in the exercise of our functions a fire and rescue authority.

As a fire and rescue authority, we have many duties and powers that describe our core functions and give us legal powers to undertake those functions. Those functions include, for example;

- Our **core functions**, as described in the Fire and Rescue Services Act 2004, that require us to give fire safety advice and prevent fires from happening; enable us to respond to fires and to

protect life and property; and to enable us to respond to road traffic accidents and other emergencies.
- A **power to respond to other eventualities** where there is a situation that may cause or is likely to cause someone to die, be injured or become ill; or that may harm to the environment (including the life and health of plants and animals).
- Our powers to **enforce and regulate fire safety law**, such as the Regulatory Reform (Fire Safety) Order 2005.

We also have **general powers** (FSA2004, Sec 5a) that enables us to do anything we consider appropriate for the purposes of the carrying-out of any of our functions or anything that is incidental to our functional purposes. This will include a power to collect, process and share personal and sensitive personal data so long as the processing is necessary for the purpose we are collecting it.

Law enforcement

During our work to enforce and regulate fire safety law, some of the personal data we collect and process will be for law enforcement purposes (as outlined in Part 3 of the Data Protection Law), which cover data processed in connection with the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Our legal basis for processing law enforcement data is that it is necessary for the performance of our functions. Our primary law enforcement functions relate to enforcement of the Regulatory Reform (Fire Safety) Order 2005 in accordance with Article 25 of the order which includes taking decisions to issue notices or to prosecute where offences have been committed and prosecution is considered to be in the public interest.

Special categories of personal data

Data protection law recognises that there are some types of personal data that are particularly sensitive and should prohibited unless the processing is absolutely necessary. This special category of data includes data revealing; racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

When it is necessary for us to process any of the special category data, it will usually be because;

- Of your employment with us (if you are an employee)
- You have already made the information manifestly public
- It is necessary to protect your vital interests or those of another person where the data subject is physically or legally incapable of giving consent
- It relates to a legal claim or legal process
- It is necessary for a task of substantial public interest and the task is within our statutory functions
- We need to identify and keep under review the equality of opportunity and treatment of different groups of people
- We are processing criminal offence data in relation to employment, public interest or to fulfil our statutory functions.

Consent

You will often have a choice about what services you receive from us, but when we collect your personal information for that service – one of our main processing activities – we will collect and retain your information because we have another duty or obligation to do so that does not require your consent. We are a public authority and we recognise that our position means that you are unlikely to be able to freely give your consent for the services we provide.

When you give us your information on the basis that you give us your consent to use it (and not because of another processing obligation we have), then you can withdraw that consent at any time. If you wish to withdraw your consent for us to use your personal data then you should contact our Data Protection Officer (see above). You should provide as much information as possible about the information you supplied, when it was given and the circumstances it was given in.

If, prior to the 25 May 2018, we have asked for, or have been given your permission to use your data and called this "consent" it is unlikely that this consent meets the standard required for UK GDPR. We are however confident that our continued use of your data is still permitted under data protection law where it falls within another legal basis, for example because it is contractual, we have a legal obligation or it is necessary for a public task. This will affect your rights (see below) and you may no longer have the right to stop us processing the information by withdrawing your previously given permission (described at the time as consent). If you have a concern about this change in processing, please contact the Data Protection Officer.

The types of information we hold

We describe the type of personal data we collect and hold by referring to "categories of personal data". The table below gives examples of the types of information that we process.

Category	**Example of data included in the category**
Personal details	Titles, names, previous names, nick-names, aliases, address, postcode, telephone numbers, email addresses, social media user names, personal websites addresses, signature, emergency contacts, family history, marital status, dependants, next of kin, language skills.
Personal features	Age, date of birth, gender, height, weight, body measurements, eye/hair/skin colour, identifying marks, images - photo/video/audio.
ID Numbers	National insurance number, passport number, driving licence number, social security number, national health number. [Note: this category may include facsimile copies of original documents containing the identifier]
Work details	Pay number, job titles, work addresses, employers name, work contact numbers, work email address, call sign, work social media user names, grade, role, rank, start date, end date, camp out base, work history, computer and communications monitoring information, lone-worker location, vehicle number plate, pager number, leave and absence, proof of right to work, building access records.
Financial details	Salary, payroll records, bank details, pension, tax, allowances, state benefits, property ownership, compensation payments.
Education	Qualification, establishment, establishment address.

Narrative data	Biography, CV, situational description, occupational experiences, behavioural characteristics, professional membership, personal references, performance evaluations, discipline or grievances, geodemographic segmentation data.
Special category data	Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Criminal offence data	Information relating to criminal offenses (alleged or proven) or personal data held with the intention of bringing about a criminal prosecution.

Publicly accessible sources

During our work, we may refer to information, including personal data, that is available on publicly accessible sources. These sources will include information made available by other public bodies, regulators and enforcing authorities (for example public registers) as well as information posted on social media, other websites and news media.

We may use information that is publicly available to inform our decisions about our work with you. That may include our dealings with you during the performance of a contract (as a supplier, a data processor or an employee) or how we provide our emergency response and other services to you, either at the time or in our planning and preparations (for example, if we are made aware of people who are at a higher risk of being involved in a fire we may try to make contact to offer prevention and safety advice).

Who we share personal information with

To fulfil our responsibilities and functions as a fire and rescue authority, it will be necessary for us to share some or all of your personal data with other organisations. When we share data we will be doing so knowing that we have legal basis to do so and that it is necessary for that purpose.

In general terms, we will only share information with another organisation where;

- They are responsible for providing services and care during emergencies
- They can help to prevent you from dying, or from becoming injured or ill, or prevent harm to the environment
- The information can be used to prevent or detect crime, including the prevention of fraud
- The information is necessary for any stage of legal proceedings
- They are processing data on our behalf and we have contract specifying the details

The categories of organisations who we might share personal data with are shown in the table below.

Category	**Example of recipients included in the category**
Emergency Services	Fire and Rescue, Police, Ambulance, Armed forces, Coast Guard, Category 1 and 2 Responders, Utility providers, Emergency care and safeguarding Charities
Local authorities	Education, Social Care, Housing, Environmental Health, Youth Service, GLA, London Assembly
Health providers	GP, Health professional, Health board or trust, National Health Service and bodies

Category	Example of recipients included in the category
Government agencies	Home Office, MOD, HMRC
Legal services	Solicitors, Law courts, Public Inquires and Inquests
Regulators	HSE, Pension Regulator, Safety Committees, Auditors
Employers & Businesses	Outside employers, Registered childcare provider, External trainers, NFCC, registered charities,
Appropriate adults	Parent, carer, family member, guardian, teacher, LFB volunteer
Contractors & suppliers ("Data processors")	Data processors are third parties who process personal data on our behalf.

Data processors

Data processors are third parties who process personal data on our behalf. These are typically the suppliers and contractors we use to provide us with good and services under contract. Occasionally, those contractors will provide services direct to you on our behalf. Examples of contractors who are our data processes include those that provide us with; recruitment support, IT systems, IT developers and engineers, telecom services, security systems, occupational health and staff wellbeing services.

We have contracts in place with all of our contracts who are also our data processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

Transfers to third countries or international organisation

We do not transfer your data outside of the UK as part of our day-to-day work. However, as IT providers become more global and IT services are provided 'in the cloud' we know that some of the data we hold is hosted on computer servers that are outside of the UK or of the European Union.

When our data processors store data outside of the area where the UK GDPR applies then the security of this information will be covered by the terms of our contract with them (or them with us). You can be assured that when this happens that you will have the same degree of protection in respect of your personal information as thought was held within the UK or the area of the European Union.

If you don't give us the information we need

You will often have a choice about what services you receive from us, but when we collect your personal information for that service we will collect and retain your information because we have another duty or obligation to do so that does not require your consent.

If you don't provide certain information when requested, we may not be able to provide you with our services (for example providing you with a fire alarm and advice) or perform the contract we have entered into with you (for example if you are an employee). We may also be prevented from putting you in touch with other organisations and services that can provide you with help, support, advice and care.

We would encourage you to provide us with the data we need to do our job, but if you have any concerns about providing your personal information when asked, please discuss those concerns with us. If you are not already in contact with a member of our staff then you can discuss those concerns with our Data Protection Officer.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. With the exception of some of our recruitment and staff management processes, we won't make decisions about you that will have a significant impact on you based solely on automated decision-making. If we use automated decision making it will be because it is necessary to perform the contract with you and we will have taken appropriate measures to safeguard your rights.

How long we keep personal information

We have a records management strategy that determines how long we keep records and information . This includes records with personal data. As a public body we need to keep records to help us plan and deliver our services, to show how we have made decisions, to prepare and defend legal claims and to maintain a historical archive of the work of the London Fire Brigade.

When deciding how long to keep information, we need to consider a number of things. These include:

- Statutory records required to be kept by law
- Documents required to assess the performance of a contract (including staff contracts)
- Records that explain how we deliver our services and who receives them
- Our obligations to be accountable and to demonstrate good governance
- Our need to defend legal claims or to take legal action
- Administration records required to carry out and record our day to day business
- Best practice for local government records keeping
- Our interest in maintaining a public archive of the work of the London Fire Brigade

Very rarely will a retention period be a set time from a fixed point, as many of our records management decisions are driven by an action or an event. For example, the records management associated with signed contracts will be triggered by the event of the contact coming to an end (e.g. contract end date plus 12 years).

Where we are holding records that contain personal data, we will have a reason and purpose to hold on to that information. If at any time you believe we are holding records for longer than necessary, you may have the right to ask us to erase that record. If you are concerned about how long we are keeping your information, then you should contact our Data Protection Officer and give them the reasons for your concern and they will investigate the matter

Your information rights and how to access the data we hold

When we use your personal data, you have rights about how that information is processed. Those rights include how you can access the information we hold, and how, in some situations, you can stop us from processing the information or have it corrected or deleted.

Under certain circumstances, you have the right to:

- Request **access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request **correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request **erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also

have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object** to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the **restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the **transfer** of your personal information to another party.

You can read more about these rights here – https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

If you would like to exercise any of your data protection rights, you should contact the Data Protection Officer using the details listed earlier in this Notice.

If you have a concern

If you are unhappy with the way that your personal data has been used or any other aspect of how we have processed your information then please let us know. In the first instance you should contact our DPO who can investigate the matter for you and take any action that is necessary.

You also have the right to raise your concern with the Information Commissioner. Details of how to make a complaint to the ICO are on their website at http://ico.org.uk or you can write to them at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Document history

Assessments

An equality, sustainability or health, safety and welfare impact assessment and/or a risk assessment was last completed on:

EIA	12/02/08	SDIA	L - 01/09/11	HSWIA	08/02/19	RA	NA

Audit trail

Listed below is a brief audit trail, detailing amendments made to this policy/procedure.

Page/para nos.	Brief description of change	Date
Throughout	References to Data Protection Act 2018 updated to Data Protection Law.	09/06/2022
Throughout	Head of Information Management updated to Head of Information Governance. Hyperlinks and typos amended.	24/07/2024
Section 7 Section 8 NEW Appendix added Appendix 4	Additional paragraph requiring SARs requests to be focused. Additional paragraph explaining that eDiscovery tools can be used for searches. Data breach reporting expanded to include the email address for reporting and a description of what should be reported. New appendix added as Appendix 3 (which moves the Privacy Notice to Appendix 4). Appendix 3 – Advice when working overseas. The section "Why we use personal information" changed and updated to align with the revised Record of Processing Activities.	06/10/2025
Appendix 2	Appendix 2 title amended to include '(the appropriate policy document)'.	06/11/2025

Subject list

You can find this policy under the following subjects.

Data protection	Regulations
Legal	

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

Considered by: (responsible work team)	**FOIA exemption**	**Security marking classification**