**Appendix 19**

INFORMATION SHARING AGREEMENT BETWEEN

**(Note: All Red Text or highlighted in Yellow needs reviewing)**

**RBKC Housing Management Service**

**Name of contractor**

**Date**

**For review Date of Review**

**Table of contents**

[1. Introduction 2](#_Toc521060205)

[2. Objective and Term of the Agreement MANDATORY 2](#_Toc521060206)

[3. Legal basis for sharing personal information MANDATORY 2](#_Toc521060207)

[4. Participating organisation(s)/department(s) to the Agreement (the ‘Permitted Recipients’) MANDATORY 2](#_Toc521060209)

[5. Purpose(s) for which information is to be shared (the ‘Agreed Purpose’) MANDATORY 2](#_Toc521060210)

[6. Types of information to be shared (the ‘Shared Personal Data’) MANDATORY 2](#_Toc521060211)

[7. Data handling requirements MANDATORY 2](#_Toc521060212)

[8. Data protection legislation and guidance 2](#_Toc521060213)

[9. Practical application of the Data Protection Legislation 2](#_Toc521060214)

[10. Accountability under this agreement: roles and responsibilities 2](#_Toc521060248)

[10.1 Authorised officer 2](#_Toc521060249)

[10.2 Designated senior officer or Contract Manager 2](#_Toc521060250)

[10.3 Staff obligations 2](#_Toc521060251)

[10.4 Review of the Agreement 2](#_Toc521060252)

[10.5 Withdrawal from the Agreement 2](#_Toc521060253)

[11 Additional Clauses OPTIONAL 2](#_Toc521060254)

[Appendix A: The Agreement contract 2](#_Toc521060255)

[Appendix B: The Data Protection Principles 2](#_Toc521060256)

[Appendix C: special categories personal Data 2](#_Toc521060257)

[Appendix D: Designated Officers 2](#_Toc521060258)

APPENDIX E: PERSONAL DATA BREACH ARRANGEMENTS 17

# Introduction

The legal basis for sharing personal information is enshrined in:

1. the General Data Protection Regulation (*(EU) 2016/679*) (“**GDPR**”), the Law Enforcement Directive (“LED”)and any national implementing laws, regulations, and secondary legislation, as amended from time to time; and
2. the Data Protection Act 2018, to the extent that it relates to processing of personal data and privacy; and
3. all applicable law about the processing of personal data and privacy

(together the “**Data Protection Legislation**”), for example the laws that govern the services you deliver.

Other legislation or regulations governing information sharing may also apply depending on the nature and scope of the data sharing initiative, including the Crime and Disorder Act, Section 5 National Health Service Act 2006, Caldicott Principles and the Local Government Act 1972.

An information sharing agreement (this “**Agreement**”) is a contractual and operational document that governs the sharing of personal data between controllers. The Agreement provides the details necessary to ensure the actual sharing of personal information complies with the Data Protection Legislation. For example, what information will be shared, why, how and with whom.

This Agreement sets out the framework for the sharing of personal data between the parties as data controllers. Each party acknowledges that one party (the Discloser) will disclose to the other party (the Recipient) shared personal data collected by the Disclosure for the purposes set out at section 2 of this Agreement.

The Agreement is to be used where the sharing of personal information is essential to the delivery of a service or project. For example:

* for directorates where, specific information needs to be shared for a particular purpose, for example a one-off research initiative
* between directorate and their service delivery partner(s), for example adult social care and their partner NHS services or a third-party contractor.

# Objective and Term of the Agreement

The overarching objective of the agreement is to allow personal data to be processed legally with third party suppliers delivering remedial works identified from Fire Risk Assessments to homes across the borough.

This Agreement shall apply from 30 January 2023. The agreement shall last for a 5 - year period, expiring on 29 January 2028.

# Legal basis for sharing personal information

Data will be processed under Public Task. RBKC has a duty to maintain our homes and meet the required standards in doing so. In Fire Risk the key statutory duty is the Regulatory Reform Order (2005).

# Participating organisation(s)/department(s) to the Agreement (the ‘Permitted Recipients’)

The Data Controller, the party that owns the data, is RBKC Housing Management. The Data Processor for this agreement will be Name of contractor.

RBKC will be responsible for ensuring an accurate and comprehensive set of data is produced and securely processed with Name of contractor.

Name of Contractor are responsible for securely storing and processing the data to ensure it is used to arrange access to properties to complete the required work. They will ensure only their employees that make the appointments receive the data, that it is processed and stored securely, and securely deleted once the work has been completed, returning any relevant personal data to the Data Controller.

# Purpose(s) for which information is to be shared (the ‘Agreed Purpose’)

The purpose for the information being shared is to allow Name of Contractor the contact details of residents for homes where access is required to complete necessary Fire Safety works.

# Types of information to be shared (the ‘Shared Personal Data’)

The only information to be shared is as detailed in this section, none of which is deemed to be special category data.

For all Tenants and Leaseholders in a block where remedial FRA work is required:

* Names of individual Residents
* Address of the individual Residents
* Contact Details: Telephone numbers
* VIRep: Summary Warning Indicator (action to take, not nature of the concern)

# Data handling requirements

The information will be processed with Name, Job Title at Name of Contractor. Information will only be shared with colleagues at Name of Contractor where their input is essential to delivery of the works.

The sharing will be for individual schemes where RBKC selects Name of Contractor to complete work within the scope of this agreement.

All parties must follow their established information security arrangements. This will include but not be limited to any emails containing personal data being sent securely to provide additional encryption and sent to Contractor contact or an alternative named colleague confirmed to be working on the individual scheme. All personal information will be securely stored electronically, and accessibility restricted to those that are completing work arranging appointments for the necessary works for the Fire Safety Works to be completed.

Each party is responsible under the relevant Data Protection legislation when processing data. If a data breach should occur the Data Breach process and responsibilities identified in Appendix E must be followed. This includes the Data Processor informing the Data Controller immediately if they suspect a data breach.

The information will be held for 48 hours post the works having been concluded. Name of Contractor will be responsible for securely disposing of all personal data at this point.

The authorising officers for the basis of this agreement are:

* RBKC Housing Management: Daniel Smith, FM Contracts Manager
* Name of Contractor: Name and Post of authorising officer

# Data protection legislation and guidance

The Data Protection Legislation governs the protection and use of personal information identifying living individuals. It gives individuals rights in relation to the handling of their personal information by organisations.

This Agreement does not seek to supersede the principles and regulatory framework that is the Data Protection Legislation, any subordinate or related legislation, orders, or judgements. In the event of conflict between any part of this Agreement and any legislative or policy requirement in place, the latter will take precedence and that part of the Agreement deemed to be in conflict will be considered suspended until the Agreement is reviewed and, if necessary, revised.

Each party shall comply with all the obligations imposed on a controller under the Data Protection Legislation.

# Practical application of the Data Protection Legislation

## The key principles of the Data Protection Legislation

The key principles of the Data Protection Legislation shall be complied with and details are available in Appendix B.

This Agreement does assist your compliance with these principles and should flow from your privacy impact assessment for the project or new service you are about to embark upon, and in certain circumstances it is mandatory for you to complete a privacy impact assessment (known as a data protection impact assessment) under the Data Protection Legislation. Please consult the Data Protection Officer’s guidance on the RBKC internet.

## Mutual Assistance

Each party to assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

* + 1. consult the other party about any notices given to data subjects in relation to the Shared Personal Data;
    2. promptly inform the other party about the receipt of any data subject access request;
    3. provide the other party with reasonable assistance in complying with any data subject access request;
    4. not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the other party wherever possible;
    5. assist each other in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
    6. notify the other party without undue delay on becoming aware of any breach of the Data Protection Legislation;
    7. at the written direction of the Discloser, delete or return Shared Personal Data and copies thereof to the Discloser on termination of this agreement unless required by law to store the personal data;
    8. use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers;
    9. maintain complete and accurate records and information to demonstrate its compliance with this clause 9.2; and
    10. provide the other party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Legislation, including the joint training of relevant staff, the procedures to be followed in the event of a data security breach, and the regular review of the parties' compliance with the Data Protection Legislation.

## Notifying data subjects of legal basis of processing

Individuals **must** be made aware that their information will be shared for the purpose of this Agreement.

Each party shall:

1. ensure that it has all necessary notices and consents in place to enable lawful transfer of the shared personal data to the permitted recipients for the purposes of this Agreement;
2. give full information to any Data Subject (individual) whose personal data may be shared under this agreement and the nature of any processing that may be undertaken. This includes giving notice that, on termination of this Agreement, personal data relating to them may be retained by or, transferred to one or more of the permitted recipients, their successors, and assignees; and
3. consult with the other party about any notices given to Data Subjects in relation to the Shared Personal Data.

Each party shall ensure that it has identified a legal basis for processing the Shared Personal Data pursuant to the Data Protection Legislation. Where a party relies on **consent** of the Data Subject, that party shall ensure that consent is freely given, specific, informed, and unambiguous, and shall have regard to the conditions relating to consent set out in the Data Protection Legislation.

Each party shall:

* + 1. process the Shared Personal Data only for the Agreed Purposes;
    2. not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;
    3. ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this agreement;
    4. ensure that it has in place appropriate technical and organisational measures, reviewed, and approved by the other party, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
    5. not transfer any personal data received from the Discloser outside the EU unless the transferor:
       1. complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint controller); and
       2. ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 GDPR; or (iii) one of the derogations for specific situations in Article 49 GDPR applies to the transfer.
  1. **Special categories of personal data**

**Special categories of personal data** include personal 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 unique identification of a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The processing of these special categories of personal data is prohibited except for in certain circumstances set out in Appendix C.

In either case where consent has been sought, it is important to note that individuals are entitled to withdraw their consent at any time. Where an individual contacts the participating organisation/department to withdraw their consent or object to the processing - subject to any exemptions that may apply - the participating organisation/department **must** advise all other parties to this Agreement and the individual’s data must not be handled for the purpose(s) of this data sharing arrangement.

## Disclosure to third parties

Personal information should only be disclosed for the purpose identified in section 4 (Purpose for which information is to be shared) and in accordance with what the individual has been told. The rights of Data Subjects are restricted in several circumstances. These include where:

* the disclosure is necessary for the purposes of actual or prospective legal proceedings, or obtaining of legal advice or establishing, exercising, or defending legal rights (Sch 2 Para 5 DPA 2018);
* the disclosure consists of information which is required by law to be made publicly available (Sch 2 Para 5 DPA 2018); and
* the disclosure is required by an enactment, rule of law or by order of the court/tribunal (Sch 2 Para 5 DPA 2018).

## Related legislation

**The Common Law Duty of Confidentiality**

The Common law duty of confidentiality may apply to a large amount of information obtained by an organisation. As a general principle the duty arises where a person receives information in situations where it is known or can be taken to be known that the information is to be treated as confidential.

Whenever information is obtained in circumstances where a duty of confidence is to be inferred, there is a legal duty to respect the confidentiality of information provided and not to disclose it to third parties without consent, unless an overriding public interest requires it. Under common law there is a duty to act reasonably and, in a manner, that is proportionate to the aim. Information obtained in confidence should not be disclosed than is necessary in the interests of the individual.

Generally, it will be possible to satisfy legal obligations under the common law duty of confidentiality if the personal information is handled in a manner that complies with the obligations as set out in the Data Protection Act.

**The Human Rights Act 1998**

The Human Rights Act prohibits interference by a public authority with the private and family life of individuals, their homes and correspondence, save where that interference is lawful and necessary in a democratic society, public safety, the protection of rights and freedoms of others, the prevention of disorder or crime and the protection of health and morals.

Interference with an individual’s privacy must not be disproportionate even where it is in pursuit of such aims as allowed by the Human Rights Act. In addition, the handling of an individual’s personal information should only be limited to pursue the objectives for which the information was collected.

### Freedom of Information Act 2000/Protection of Freedoms Act 2012 (part 6: freedom of information and data protection)

### The Freedom of Information Act (FOIA) provides for a general right of access to official information held by public authorities (subject to the exemptions contained in the FOIA), and as each of the partners is a public authority there is a statutory duty to handle requests for information in accordance with the framework of the FOIA. Where the data sharing Protocol involves another public authority(s), it will be the duty of the recipient public authority to handle the request in accordance with the legislation. Each signatory should make proper arrangements to enable information to be shared and disclosed in relation to non-personal data.

The Protection of Freedoms Act (part 6) extends the FOIA in the following ways for the UK:

* section 102: the release and publication of datasets held by public authorities
* section 103: definition of “publicly owned company”

# Accountability under this agreement: roles and responsibilities

## Authorised officer

This Agreement must be signed by the RBKC Information Asset Owner or Director for each participating or the lead directorate and partner organisation (see Appendix A).

## Designated senior officer or Contract Manager

Each Authorised Officer to nominate at least one senior officer in for each participating or the lead directorate in RBKC and partner organisation responsible for agreeing amendments to the Agreement, monitoring and reviewing its operation and ensuring compliance. Designated senior officers and contact details are listed at Appendix D.

## Staff obligations

It is the responsibility of each participating organisation/department to ensure that staff with authorised access to the data covered by this Agreement are aware of their obligations under the Data Protection Legislation to safeguard that information. Staff should be aware that breach of the controls contained within this Agreement could be a matter for disciplinary action and may provide grounds for a complaint under the Data Protection Legislation against them which may result in criminal or civil action against them.

## Review of the Agreement

All elements of this Agreement will be reviewed every 12 months.

## Withdrawal from the Agreement

If any party wishes to withdraw from this Agreement, they must give six weeks written notice of this intent. Letters will be addressed to the signatories of the Agreement at the addresses shown in Appendix A. Individuals whose data has been hitherto shared must be informed where a participating organisation/department has withdrawn from the data sharing arrangement.

Any Party who withdraws **must** ensure that all data is reviewed and deleted.

# Appendix A: The Agreement contract

**RBKC** information sharing agreement between

RBKC Housing Management

Contractor Name

We, the undersigned, do hereby agree to implement the full range of measures outlined in this Agreement.

For and on behalf of RBKC (Housing Management)

Signature:

Name: Daniel Smith

Position: FM Contracts Manager

Address: The Network Hub, Unit A, 292 Kensal Road

London

W10 5BE

Date:

For and on behalf of Name of Contractor

Signature:

Name:

Position:

Address:

Date:

# Appendix B: The Data Protection Principles

Article 5 of the General Data Protection Regulation sets out the key principles relating to the protection of personal data and is replicated below. You should consider whether any other legislation (including the LED or Data Protection Act 2018) applies to your project and ensure compliance with the key principles set out in such legislation.

1. Personal data shall be:
   1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
   3. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
   4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
   5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
   6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

# Appendix C: Processing of special categories of personal data

1. Processing of personal 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 unique identification of a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
   1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
   2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law as far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
   3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
   4. 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 the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
   5. processing relates to personal data which are manifestly made public by the data subject;
   6. processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
   7. processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
   8. 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 based on Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
   9. processing is necessary for reasons of public interest in 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, based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
   10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, about the processing of genetic data, biometric data or data concerning health.

# Appendix D: Designated Officers

|  |  |  |  |
| --- | --- | --- | --- |
| **PARTICIPATING ORGANISATION/DEPARTMENT** | **NAME OF DESIGNATED OFFICER** | **POSITION AND RESPONSIBILITY** | **CONTACT DETAILS** |
| RBKC | Daniel Smith | FM Contracts Manager | [Daniel.Smith3@rbkc.gov.uk](mailto:Daniel.Smith3@rbkc.gov.uk) |
| Name of Contractor | Name of Contract Officer | Position of Contractor Officer | Contractor Officer Email address |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# APPENDIX E – PERSONAL DATA BREACH ARRANGEMENTS

*A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.*

*All Partners will maintain a robust data breach detection, investigation and internal reporting procedure and have due regard to the guidance of the Information Commissioner’s Office (ICO).*

*If a Partner has a data breach it will:*

* *Inform all Partners and identify any urgent remedial actions required that might affect other Partners*
* *take steps to establish the likelihood and severity of the resulting risk to affected data subjects including the risk of physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of Pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*
* *Inform the Head of Home Ownership of the steps it is taking to establish the likelihood and severity of the risk and keep the Head of Home Ownership informed of progress.*
* *If it’s likely that there will be such a risk to data subjects rights and freedoms the Partner will notify all other Partners and the ICO (within 72 hours where feasible) and inform those individuals affected without undue delay;*
* *In all cases the Partner will keep full written records of any data breach, its investigation, the remedial steps taken and the reasons for such steps.*
* *All Partners affected by a data breach will share with other Partners a lesson learned analysis of the cause and effects of reportable data breaches and this Appendix H will be reviewed after every such data breach.*

*Each Partner is individually liable for any fine or penalty imposed on it by the ICO and for any loss or damage recovered against it by whatever means by any person in connection with a data breach.*