Northwards Housing
North Manchester's Council Homes

DATA PROTECTION POLICY

CONTENTS

1. INTRODUCTION

1.1 This policy sets out how Northwards Housing handle personal data, whether that be information about our tenants, suppliers, employees or other third parties. Our policy takes into account the changes introduced by the General Data Protection Regulation ("The GDPR") and the Data Protection Act 2018.

1.2 This policy applies to all staff. Data protection is a collective responsibility and all staff are required to demonstrate good data protection practices to support Northwards in creating a strong culture of data protection compliance. Further guidance for employees can be found at Appendix 2. Any breach of this policy may result in disciplinary action and, where data processors and sub-processors are concerned, termination of our relationship.

2. SCOPE

2.1 Northwards recognises that the correct and lawful treatment of personal data is important to our success as a business and to ensure that those whose personal information we process have confidence in us. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

2.2 We have appointed a Data Protection Officer ("DPO") who is responsible for overseeing this policy. The DPO is HY Professional Services ("HY") who can be contacted as follows:-

In writing: HY, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL
By email: DPO@wearehy.com
By telephone: 0161 804 1144.

2.3 Please contact the DPO with any questions about the operation of this Policy.

3 JARGON BUSTER

3.1 For those who are not familiar with the terminology used under data protection laws, we have set out in Appendix 1 a number of definitions of terms used in this policy.

4. DATA PROTECTION PRINCIPLES

4.1 We will comply with the data protection principles set out under the GDPR when processing personal data. We will ensure that personal data is:-

(a) Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
(b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
(d) Accurate and where necessary kept up to date (**Accuracy**).
(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

4.2 We will demonstrate our compliance with the data protection principles listed above (**Accountability**).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

Lawful Processing

5.1 Personal data must be processed lawfully. Under the GDPR, there are a number of 'bases' which make it lawful to process personal data. We will only process personal data if one or more of the following apply:-

(a) the data subject has given his or her **Consent**.
(b) the processing is necessary for the **performance of a contract** with the data subject.
(c) to meet our **legal obligations**.
(d) to protect the data subject's **vital interests**.
(e) to carry out a **Public Task.**
(f) to pursue our **legitimate interests** for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and

freedoms of data subjects. Information will only be processed under this basis in rare circumstances.

5.2 We recognise that some categories of personal data are more sensitive and further conditions must be satisfied if we are to process this information. This includes information about an individual's race, ethnic origin, political opinions, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation. Where we process this type of information, we will ensure that we do so in accordance with the GDPR and data protection laws.

Consent

5.3 Where consent is the lawful basis for processing, we recognise that under the GDPR, there are stricter rules about how this is obtained. If we do need to obtain consent, we will ensure that:-

(a) the data subject either by a statement or positive action gives their consent.
(b) consent is not inferred by silence.
(c) pre-ticked boxes are not used as a means of obtaining consent.
(d) consent is separated from other documents such as terms and conditions or contracts.
(e) data subjects are able to withdraw consent to processing at any time.

5.4 The above rules ensure that data subjects give their consent freely, understand what they are consenting to and can change their mind should they wish to do so.

5.5 We will make guidance available to staff in relation to obtaining consent as appropriate.

5.6 We will keep appropriate records evidencing how we obtain consent.

Transparency

5.7 We are required to provide detailed and specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. We will provide this information by publishing a privacy policy on our website which will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand it.

6. PURPOSE LIMITATION

6.1 We will only collect personal data for specified, explicit and legitimate purposes.

6.2 We will not use personal data for new, different or incompatible purposes from those disclosed when it was first obtained, unless we have informed the data subject of the new purposes and they have consented where necessary.

7. DATA MINIMISATION

7.1 We will ensure that the personal data which we process is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. We will achieve this

in the following ways:-

(a) Staff will only process personal data when performing duties which require its use.
(b) We will not collect excessive data and only process data that is necessary to complete a task.
(c) When we no longer require the data, we will delete it in accordance with our retention procedures.

8. ACCURACY

8.1 We will take all reasonable steps to ensure that personal data that we hold is accurate and, where necessary, kept up to date. Where we identify inaccuracies, we will correct or delete it without delay.

8.2 We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

9. STORAGE LIMITATION

9.1 We recognise that personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 We will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

9.3 We will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with our records retention schedules and policies.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

Protecting Personal Data

10.1 We recognise that personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

10.2 We will develop, implement and maintain safeguards to ensure that personal data which we process is kept secure and confidential. We will evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

10.3 All our employees will follow all the procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

10.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who have a need to know and are

authorised to use the personal data can access it.

(b) **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users are able to access the personal data when they need it for authorised purposes.

Reporting a personal data breach

10.5 We recognise that the GDPR requires Controllers, in some circumstances, to notify a personal data breach to the Information Commissioners Office and, in certain instances, the data subject.

10.6 We will put in place data breach procedures to deal with any suspected personal data breach. Where our employees suspect that a personal data breach has occurred, they will follow our personal data breach reporting procedure (Appendix 3) and notify the DPO.

11. TRANSFER LIMITATION

11.1 We recognise that the GDPR restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

11.2 We will only transfer personal data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects rights and freedoms.

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism.

(c) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1 We recognise that data subjects have rights when it comes to how we handle their personal data. In particular, data subjects have a right to access information which we hold about them. We will respect these rights when processing personal data and maintain procedures for handling subject access requests (Appendix 4).

13. ACCOUNTABILITY

Accountability

13.1 The GDPR requires usto implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

13.2 To demonstrate our compliance with the data protection principles, we will do the following:-

(a) appoint a suitably qualified DPO.
(b) develop appropriate and relevant policies, privacy information and procedures.
(c) implement privacy by design when processing personal data.
(d) completing DPIAs where processing presents a high risk to rights and freedoms of data subjects.
(e) providing training to staff
(f) undertake information audits.
(g) Providing appropriate training.

13.3 We will maintain a record of processing activities in accordance with the GDPR.

Privacy by design and data protection impact assessment (DPIA)

13.4 We will implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with the data protection principles.

13.5 We will conduct DPIAs in respect of high risk processing. In particular, we will conduct a DPIA when implementing a major system or change programs involving the processing of personal data.

13.6 The DPO will be consulted when carrying out a DPIA. The DPIA will include:

i. a description of the processing, its purposes and the data controller's legitimate interests if appropriate.
ii. an assessment of the necessity and proportionality of the processing in relation to its purpose.
iii. an assessment of the risk to individuals; and
iv. the risk mitigation measures in place and demonstration of compliance.

14. DIRECT MARKETING

14.1 We recognise that we are subject to certain rules and privacy laws if we send marketing communications. We will ensure that our marketing communications comply with these laws at all times.

15. SHARING PERSONAL DATA

15.1 We will not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

15.2 We will only share personal data we hold with another employee or representative if they have a job-related need to know.

15.3 We will only share personal data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services.

(b) sharing the personal data complies with the privacy policy provided to the data subject and, if required, the data subject's consent has been obtained.

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

(d) a fully executed written contract that contains GDPR approved third party clauses has been obtained where required.

15.4 We may share personal data as part of the National Fraud Initiative with other public bodies, as appropriate, for the detection and prevention of fraud. We also share information with Greater Manchester Police and Manchester City Council where it is lawful and necessary in the prevention, investigation and detection of crime or anti-social behaviour and in order to safeguard children or vulnerable adults.

16. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time and will communicate any changes to you accordingly.

APPENDIX 1 – JARGON BUSTER

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. Northwards is a Data Controller. We are responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Personnel and Personal Data which we collect as part of our activities.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design. We will carry out a DPIA for all major system or change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): Northwards is required by law to appoint a DPO. The DPO must have expertise in data protection laws and carry out certain data protection related tasks set out in law.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

ICO: Information Commissioner's Office is the UK's independent regulatory body set up to uphold information rights.

Personal Data: any information identifying a Data Subject.

Personal Data Breach: a breach of security, confidentiality or integrity of Personal Data. The loss, or unauthorised access or disclosure of Personal Data is a Personal Data Breach.

Personnel: all employees, workers, independent contractors, agency workers, consultants, directors, volunteers and others.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Policies or Privacy Notices: documents provided to Data Subjects when we collect information about them explaining how we use their Personal Data.

Processing or Process: any activity that involves the use of Personal Data. It includes collecting, recording, holding, organising, amending, retrieving, using, disclosing, erasing or destroying it.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

APPENDIX 2 – GUIDANCE FOR EMPLOYEES

1. All personnel at Northwards should take steps to promote good practice and create a strong culture of data protection compliance. We have set out below some guidance which will enable you to do this.

Keeping Personal Data Secure

2. We require you to work in a way which is secure. This will prevent unauthorised access or loss of personal data. Some of the things that you can do include the following:-

    a. Ensure that paper files and other manual records containing personal data are held securely.
    b. Ensure that personal data held on computers, systems and mobile devices are password protected.
    c. You should periodically change your passwords.
    d. Where electronic personal data is accessed on computers or laptops when out of the office, these should be encrypted.
    e. Where sensitive personal data is regularly shared between Northwards and an external provider / partner, you should use more secure methods of transfer via our cloud-based platforms (e.g. Sharepoint).
    f. Ensure that unencrypted CD's and USB devices are not used.

If you receive a request for disclosure of Personal Data

3. If you receive a request for the disclosure of personal data from an individual which we hold about them, then this is known as a **Subject Access Request (SAR).** There are different types of requests that can be made. Where you receive a SAR, you must deal with it in accordance with Northwards SAR Procedure (Appendix 4).

If you become aware of a Personal Data Breach

4. If you become aware of a Personal Data Breach, you must report follow the procedure outlined in 10.5 and 10.6 of this policy and Appendix 3 below.

Clear Desk Policy

5. During the working day, work will not be left unattended on desks for long periods. At the end of each day, every desk will be cleared of all documents that contain official information, or any information relating to individuals. Personal information about individuals will not be left in in-trays and work will be stored in a desk drawer, cupboard or cabinet. Sensitive or Special Category information will always be locked away.

6. Each Head of Service is responsible for implementing the policy within their service area in the most practicable way possible.

7. Any information left in the top tier of an in-tray at the end of the working day must be suitably covered with a file or folder so that the contents of the in-tray are hidden from view

(this excludes personal information about individuals which must be stored away and never left in in-trays).

8. Files or folders are permitted to be left on desks for ease of access, providing they are tidy and don't contain personal information about individuals or sensitive information.

APPENDIX 3 – PERSONAL DATA BREACH REPORTING PROCEDURE

The General Data Protection Regulation ("GDPR") places reporting obligations on us, as a data controller, in the event of a personal data breach. This procedure is to ensure that appropriate action is taken in a timely manner to comply with the requirements of the GDPR.

This procedure applies to all staff, board members and volunteers. You must read, understand and comply with this procedure in the event of a personal data breach. It is important to understand what constitutes a data breach and to feel comfortable in reporting it. Our priority is always the protection of data, rather than fear or blame, so that swift action is taken to preserve the rights and freedoms of those who trust us to handle their data. For that reason, any failure to follow this procedure may result in disciplinary action.

This procedure should be read in conjunction with our Data Protection Policy, in particular section 10.

1. Personal Data Breach

1.1 All staff must notify their line manager and the Head of Business Effectiveness & Communications immediately on becoming aware of a personal data breach. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1.2 The DPO will be notified of all data breaches by the Head of Business Effectiveness & Communications.

1.3 If the Head of Business Effectiveness & Communications is unavailable then the DPO and a Director must be notified directly.

1.4 Third-party processors and sub-processors must also immediately report to Northwards that a data breach has occurred. We will work with the processor to investigate the breach and report (where necessary) to the ICO. It is not the processor's responsibility to report to the ICO.

2. Investigation

2.1 The DPO will support Northwards to immediately investigate the personal data breach reported, taking such steps as are reasonable to identify the following:-

(a) How the breach occurred

(b) When the breach occurred

(c) Whether the breach is likely to result in a risk to the rights and freedoms of data subjects

(d) Whether the Information Commissioners' Office should be notified

(e) Whether the data subject(s) should be notified

(f) Any other matters to be investigated at the direction of the DPO

3. Record of Breach

3.1 The data controller and the DPO will document the personal data breach in the Data Breach Record.

3.2 If, following investigation, the DPO determines that the "Reporting Threshold" has not been passed, this decision will be recorded, and the incident closed.

4. Reporting Threshold

4.1 The DPO, in consultation with the Head of Business Effectiveness & Communications, will be responsible for determining whether or not the threshold for notifying the ICO has been met. The DPO will make this decision and record it taking into account relevant laws and guidance.

5. Notification of a personal data breach to the ICO

5.1 The DPO will ensure that a personal data breach is reported to the ICO not later than 72 hours after Northwards became aware of the breach using the letter template below at notification 1 if the "Reporting Threshold" has been met.

5.2 Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

5.3 If a notification to the ICO is made, the DPO will ensure that appropriate steps are taken to fully co-operate with their requests / investigations.

6. Notifying the data subject(s)

6.1 Subject to 6.2, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject(s) the DPO will ensure that steps are taken by Northwards to notify the data subject as soon as possible using letter template below at notification 2.

6.2 A personal data breach is likely to result in a risk to the rights and freedoms of those to whom the personal data breach relates if it has a significant detrimental impact on individuals – examples include discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. However, this has to be assessed on a case by case basis by the DPO.

6.3 The data subject need not be notified if any of the following apply:-

(a) Northwards has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular, those that ensure the personal data is unintelligible to any person who is not authorised to access it, such as encryption

(b) Northwards has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to at 6.1 and 6.2 is no longer likely to materialise

(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

Notification 1 - template to be adapted to suit specific circumstances

The Information Commissioners' Office
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[Date]

Dear Sirs,

Notification of a Personal Data Breach in accordance with Article 33 of the General Data Protection Regulation ("GDPR")

We write to the Information Commissioners' Office ("ICO") in accordance with Article 33 of the GDPR to provide notification of a personal data breach. It is considered that the breach is notifiable on the basis that it is likely to result in a risk to the rights and freedoms of those affected.

[We are aware that notification should be made to the ICO by no later than 72 hours after having become aware of the personal data breach. Unfortunately, we were unable to comply with this requirement for the following reasons XXXXXX].

The nature of the personal data breach, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

[INSERT DETAIL]

Name and contact details of the Data Protection Officer

[INSERT DETAIL]

The likely consequences of the personal data breach

[INSERT DETAIL]

Measures taken or proposed to be taken to address the personal data breach

[INSERT DETAIL]

We look forward to your office contacting us shortly to inform us of the next stage of the process.

Yours sincerely,

For and on behalf of

Northwards Housing
Notification 2 – template to be adapted to suit specific circumstances

[Name]
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[Date]

Notification of a Personal Data Breach

We write to you to advise you of a recent personal data breach within Northwards Housing. Having considered the nature of the breach, we have reported this to the Information Commissioners' Office ("ICO") who will advise us of the next steps in its process. The ICO is the UK's independent body set up to uphold information rights.

The purpose of this letter is to provide you with information about the personal data breach, how it occurred, who it has affected, the type of information which the breach relates to, the consequences of the breach and the measures we have taken to address the breach.

The nature of the personal data breach, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

[INSERT DETAIL]

Name and contact details of the Data Protection Officer

[INSERT DETAIL]

The likely consequences of the personal data breach

[INSERT DETAIL]

Measures taken or proposed to be taken to address the personal data breach

[INSERT DETAIL]

Clearly, we appreciate that you will be concerned about the personal data breach. On behalf of Northwards, we sincerely apologise for any distress that this may cause and can assure you that we are taking all necessary steps to address the situation. Should you wish to discuss this matter with our Data Protection Officer, then please feel free to do so by telephone [Telephone number] or email [email address].

Yours sincerely,

For and on behalf of
Northwards Housing

APPENDIX 4 – SUBJECT ACCESS PROCEDURE

1. ABOUT THESE PROCEDURES

1.1 Northwards holds personal data about a variety of individuals. For example, we hold personal data about our tenants and staff. These individuals are referred to as "data subjects" and have certain rights in respect of their personal data. When we process a data subjects' personal data, we shall respect those rights.

1.2 These procedures provide a framework for responding to the different types of requests for personal data that we may receive. If you are unsure about how to respond to a particular request, you should seek advice from the Governance Support Manager or the Head of Business Effectiveness & Communications or the Data Protection Officer (DPO) by telephone (01706 399905) or by email (DPO@wearehy.com).

1.3 These procedures only apply to requests for personal data which we process about a data subject.

2. RESPONDING TO REQUESTS TO ACCESS PERSONAL DATA

2.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR we will take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) send an acknowledgement to the individual requesting access to their personal data.

(c) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity.

(d) If the request is vague or unclear, we will ask for greater clarification so that we can comply with the request.

(e) search databases, systems, applications and other places where the personal data which are the subject of the request may be held.

2.2 If personal data is held, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a) the purposes of the processing;

(b) the categories of personal data concerned (for example, contact details or bank account information);

(c) Who we have or may share it with;

(d) where possible, the envisaged period for which the personal data will be stored;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO);

2.3 We shall also, unless there is an exemption (see section 8 below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within **one month** of receipt of the request. If the request is complex we may extend the period for responding by a further **two months**. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

2.4 Before providing the personal data, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to disclosing it, unless those other data subjects have consented to the disclosure of their personal data.

2.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

2.6 If we are not going to respond to the SAR, we shall inform the data subject of the reason(s) for this and of the possibility of lodging a complaint with the ICO. Before refusing to respond, the Head of Business Effectiveness & Communications must be consulted.

3. RESPONDING TO REQUESTS TO RECTIFY PERSONAL DATA

3.1 Data subjects have the right to have their inaccurate personal data rectified. For example, we might hold an incorrect telephone number about a tenant. Where such a request is made, we shall, unless there is an exemption (see section 8 below), rectify the personal data without undue delay.

3.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data has been disclosed (for example, our third-party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort.

4. RESPONDING TO REQUESTS FOR THE ERASURE OF PERSONAL DATA

4.1 Data subjects have the right, in certain circumstances, to request that we erase personal data that we hold about them. Where such a request is made, we shall, unless there is an exemption (see section 8 below), erase the personal data without undue delay if:

(a) If we no longer need the personal data for the purpose we collected it

(b) the data subject withdraws their consent to us processing the personal data and consent was the legal basis for processing.

(c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests. However, if we have compelling grounds which override the data subject's rights, the request should be refused.

(d) the data subject objects to the processing of their personal data for direct marketing purposes.

(e) the personal data has been unlawfully processed.

(f) the personal data has to be erased for compliance with a legal obligation to which we are subject.

4.2 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see Para 4.5 and section 8 below), take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;

(c) If the request is vague or unclear, we will ask for greater clarification so that we can comply with the request.

(d) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within **one month** of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further **two months**. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

(e) where we have made the personal data public, we must, taking reasonable steps, including technical measures, to inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and

(f) communicate the erasure of the personal data to each recipient to whom the personal data has been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

4.4 If we are not going to respond to the request, we shall inform the data subject of the reasons for this and of the possibility of lodging a complaint with the ICO. Before refusing to respond, the Head of Business Effectiveness & Communications must be consulted.

4.5 In addition to the exemptions in section 8 below, we can also refuse to erase the personal data to the extent processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which we are subject;

(c) for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

(d) for reasons of public interest in the area of public health;

(e) for the establishment, exercise or defence of legal claims.

5. RESPONDING TO REQUESTS TO RESTRICT THE PROCESSING OF PERSONAL DATA

5.1 Data subjects have the right, unless there is an exemption (see section 8 below), to restrict the processing of their personal data if the circumstances when we may receive such a request include when:-

(a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

(b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) we no longer need the personal data for the purposes we collected it, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

(d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

5.2 Where processing has been restricted, we shall only process the personal data (excluding storing them):

(a) with the data subject's consent;
(b) for the establishment, exercise or defence of legal claims;
(c) for the protection of the rights of another person; or
(d) for reasons of important public interest.

5.3 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

5.4 We shall communicate the restriction of processing to each recipient to whom the personal

data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

6. RESPONDING TO REQUESTS FOR THE PORTABILITY OF PERSONAL DATA

6.1 Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, you should seek advice from the DPO.

7. RESPONDING TO OBJECTIONS TO THE PROCESSING OF PERSONAL DATA

7.1 Data subjects have the right to object to the processing of their personal data. This may occur where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us. For example, we may hold information about our tenants which is necessary to perform our functions but which they for some reason object to. Where an objection is received, we must consider whether our own interests in processing the personal data outweigh the rights of the data subject. You should seek advice from the DPO if you receive such a request.

7.1 Where personal data is processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data. If a data subject makes such a request, we shall stop processing the personal data.

8. EXEMPTIONS

9.1 Before responding to any request, we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) other important objectives of general national public interest
(f) the protection of the data subject or the rights and freedoms of others; or
(g) the enforcement of civil law claims.