# Data Subject Rights Request Procedure

| | |
|---|---|
| **SUMMARY:** | Data Subject Rights Request Procedure |
| **VERSION** | 1.1 |
| **DATE ISSUED:** | October 2019 |
| **AUTHOR:** | Susan Campbell |

| DISTRIBUTION | |
|---|---|
| **NAME** | **ORGANISATION** |
| File & All Employees | **Hanover (Scotland) Housing Association Ltd** |
| Provided as required | **Data Subjects** |

# Contents

**Contents** ..... **4**

**1 Introduction** ..... **5**

**2 Background** ..... **5**

2.1 What is Personal Data? ..... 5

2.2 Rights of the Data Subject ..... 5

**3 General Procedures** ..... **8**

3.1 Initial Request and Response ..... 8

3.2 Internal Process ..... 10

3.3 Completion of Request ..... 11

**4 Specific Rights** ..... **12**

**5 Exemptions** ..... **17**

**6 Sanctions and Repercussions** ..... **18**

**7 Planning and Deadlines** ..... **20**

**8 Document Control** ..... **21**

# 1 Introduction

In accordance with the General Data Protection Regulation and the UK Data Protection Act 2018, data subjects are conferred certain rights with regards to their personal data. This Procedure states these rights, how they may be exercised by a data subject, and the procedures for Hanover (Scotland) Housing Association Ltd] to follow when these situations arise.

# 2 Background

## 2.1 What is Personal Data?

Personal data means any information about a living individual ("data subject") from which that person can be identified, whether directly (e.g., personally identifiable information such as a name) or indirectly (e.g., online identifiers such as IP address or cookies). It does not include data where the identifying element has been removed (anonymous data).

## 2.2 Rights of the Data Subject

Data subjects have the following rights in relation to their personal data:

| RIGHT | EXPLANATION |
|---|---|
| Access | The right to obtain a copy of the personal data that we hold on the data subject. |
| Rectification | Where data that we hold on a data subject is incorrect or incomplete, data subjects have the right for this to be corrected. |
| Erasure | In the following circumstances data subjects may request the deletion of their data:<br>• Where it is no longer necessary for the original purpose<br>• Where consent was previously given and the data subject wishes to withdraw it<br>• Where the data subject objects to the processing of their data, and we have no overriding legitimate interest to continue this processing<br>• The data subject no longer wishes their personal data to be used for direct marketing |

| RIGHT | EXPLANATION |
|---|---|
| | • To meet a legal obligation<br>• Where personal data is unlawfully processed<br>• We have processed the personal data in relation to providing services to a child |
| Restriction of processing | In the following circumstances data subjects have the right to request us to restrict how we process their data:<br>• They dispute the accuracy of the personal data that we hold on them<br>• The processing is unlawful and they wish us to restrict processing instead of deleting their data<br>• We no longer need to process their data, but the data is required by the data subject in relation to legal claims<br>• In relation to the data subject raising an objection to the processing of their data |
| Data portability | The data subject has the right for their data to be transferred to another controller if we process their data by automated means, and where processing is on the basis of consent or as part of a contract with the data subject. |
| Object to processing | The data subject may object to processing of their data where:<br>• Where it is an absolute right<br>  ○ In relation to direct marketing or profiling purposes<br>• Where it is not an absolute right and the data subject must give specific reasons why they are objecting to one of the following:<br>  ○ Processing personal data for scientific or historical research, or statistical purposes<br>  ○ A task carried out in the public interest<br>  ○ The exercise of official authority vested in the data controller<br>  ○ Our legitimate interests (or those of a third party) |

| RIGHT | EXPLANATION |
| --- | --- |
| | • Unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims<br><br>Note the law on the right to object is complex and no decision should be made on the applicability or otherwise of this right without consulting the Director of Organisational Services |
| | |

# 3 General Procedures

The sub-sections that follow apply to all rights requests. Instructions pertaining to specific rights can be found in Section 4. In normal operation, the Director of Organisational Services is responsible for coordinating internal activities and the response to the data subject. In the event that he/she is unavailable (e.g., holidays or sickness), a member of the management team will enact the tasks stated in this procedure.

## 3.1 Initial Request and Response

### 3.1.1 Request

A data subject may initially raise a request by any available channel (e.g., by email, phone, in conversation with a member of staff, using social media) and does not have to include the phrase 'subject access request' or quote relevant legislation as long as they make it clear they are asking about their own personal information. However, we require a formal record of this request to be made either in writing or by email, and the Director of Organisational Services must be made aware of these as soon as possible. These are the approaches the data subject should be encouraged to take:

1. To contact the Director of Organisational Services directly
    a. By email at dataprotectin@hanover.scot
    b. Or by post: 95 McDonald Road, Edinburgh, EH7 4NS

If the data subject does not wish to submit their request using either of these methods, the member of staff receiving the request must forward it to the Director of Organisational Services by suitable internal methods, without delay.

It is not mandatory for the data subject to use a specific request form and at present Hanover does not provide one. However, the information we require is:

- Name
- Any other identifier used
- Contact details
- The nature of the request, i.e., the type and/or subject of information required
- The date range for the request, i.e., last 3 years, between 2012 to present, etc.
- Is this the first time the request has been made?

### 3.1.2 Response

The Director of Organisational Services must record the request in the Rights Request Log. completing all required fields as necessary; throughout this procedure the log must be updated until the request is complete. The Director of Organisational Services must contact the data subject without undue delay to inform with an initial response as follows:

- State that the request has been logged
- Whether any verification of identity is required
- Whether any fee will be charged
- The timescales for the completion of the request

Our internal target for the initial reply to the data subject is 72 hours from the point at which the request is received.

### 3.1.3 Verification of Identity

All reasonable steps will be taken to verify the identity of the data subject. We may request a copy of a suitable identity document (e.g., passport, driving licence, utilities bill). The Director of Organisational Services will determine if additional verification is required on a case-by-case basis and must ensure any verification steps are proportionate to the amount and sensitivity of personal data in scope.

If the request is not from the data subject, but a party with authorisation to act on their behalf, this party will need to provide evidence of their identity, the data subject's identity and authorisation of their ability to act on the data subject's behalf. Authorisation from the data subject to act on their behalf may include a signed letter declaring authorisation, a letter of authority, lasting or Enduring Power of Attorney, or evidence of parental responsibility.

### 3.1.4 Fees

Data subjects will not normally have to pay a fee to exercise any of their rights. However, we may charge a reasonable fee for the administrative costs of complying if the request is clearly unfounded or excessive, or the request is a duplicate of one previously received from the data subject. Any decision on charging a fee will be agreed by the Director of Organisational Services.

No fee amount is set in law so if a fee is charged it is necessary to be able to justify the amount.

### 3.1.5 Timescales

All requests should be met without undue delay, and at most within one month.

Calculate the time limit from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, the date to respond will be the previous working day.

In the case of complicated requests or those involving a large volume of data or requests, this may be extended by a further two months, but the data subject must be informed of this extension within a month of the request being received, along with reasons for the extension.

Although sufficient confirmation of the data subject's identity must be received, lack of this is not a reason to delay acting on the request. Instead, the request must be actioned but the response delayed until immediately after the identity is confirmed.

## 3.2 Internal Process

### 3.2.1 Initial Evaluation

Once the request has been lodged and an initial response provided to the data subject, the Director of Organisational Services will coordinate with the Operational Manager involved and other relevant staff to determine whether the request can be met. This decision must be made within one week of the request being made.

If the data subject cannot be identified, or the request is unfounded or excessive, we may refuse to act on the request. In this case, the Director of Organisational Services must inform the data subject of this without undue delay and at the latest within one month from the date of the request, and state the reason for the refusal, and provide information on lodging a complaint with the supervisory authority (3.3.2) and the possibility of seeking a judicial remedy.

Note it is necessary to begin the process of responding (see Section 4) as soon as the request is received and before identification is complete, unless it is impossible to explicitly identify the data subject from the information received.

## 3.3 Completion of Request

### 3.3.1 Method of Communication with Data Subject

For ongoing communication prior to the final response:

If possible use email to ensure a record of the communication is kept. If the data subject has not communicated electronically and has not provided an email address use the same method they employed to submit their request.

For delivery of the final response:

Where the data subject has made the request by electronic means, and unless otherwise requested by the data subject, the information should be provided in a commonly used electronic form. Otherwise the information will need to be printed and posted.

### 3.3.2 Complaints

If we determine that a request cannot be met, use the following text in the response to the data subject:

> If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.
>
> You can contact them by:
>
> - Call 0303 123 1113
> - Online at www.ico.org.uk/concerns
>
> If you are based outside the UK, you have the right to lodge your complaint with the relevant data protection regulator in your country of residence. If in doubt, contact the ICO.

The data subject also has the option to seek to enforce their rights through a judicial remedy. If this situation arises the Director of Organisational services should consult legal counsel.

# 4 Specific Rights

### 4.1.1 Access to Personal Data

The data subject is exercising their right to obtain a copy of the personal data that we hold on the data subject.

1. If possible establish the relationship we have with the data subject; are they a current or ex-employee, a supplier, a client?
2. Use the record of processing  preadsheet to ascertain what information we're likely to hold and the storage location(s).
3. Confirm with relevant managers (i.e., line managers, HR, account managers) whether they hold any information on the data subject elsewhere, such as in email folders.
4. Create a copy of all the relevant personal data we hold about the data subject and store this in a secured location using the data subject's name as the folder name.
5. Do not change the data; the information provided must be what was there at the time of the request.
6. Check the data to ensure none of the exemptions are applicable (see Section 5).
7. Confirm the data subject has been identified correctly.
8. Provide the data in the correct format with reference to Section 3.3.1 above, together with confirmation of the processing activities and a copy of the relevant privacy notice.
9. Complete the relevant fields in the Rights Request log.
10. Remove the copy of the personal data stored in the location used in step 4.

### 4.1.2 Right to Rectification of Personal Data

The data subject is exercising their right to have incorrect or incomplete information corrected. Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data we hold.

If the data in question records an opinion, it is, by its very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

If the personal data is contained within an historical record and was accurate at the time, it is possible to argue that updating it will render it inaccurate. However, there must be a valid legal basis for processing historical personal data.

1. Complete steps 1 to 3 under Section 4.1.1 unless already done so.
2. If not clear, confirm with the data subject the information which is incorrect or incomplete.
3. Advise the data subject they have the right to request restriction of the processing of their personal data while we are dealing with their request; however, if we believe we have a compelling reason for not doing so we will inform them of this decision and the reason(s) for it. Otherwise as a matter of good practice, we will restrict the processing of the personal data in question while we are confirming their request, whether or not the data subject has exercised this right (refer to Section 4.1.4.).
4. As the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data, we will identify the most appropriate method of restriction for the type of processing we are carrying out.
5. Take reasonable steps to ensure that the new information provided by the data subject is accurate. The steps taken to check accuracy will depend on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort that must be put into checking its accuracy.
6. Confirm the data subject has been identified correctly.
7. Rectify the incorrect or incomplete information.
8. Inform any third parties or data processors who have a copy of the information of the changes made.
9. Provide information to the data subject of the actions taken, with reference to Section 3.3.1 above, on the changes made, together with confirmation of the processing activities and a copy of the relevant privacy notice.
10. Complete the relevant fields in the Rights Request log.

### 4.1.3 Right to Erasure of Personal Data

The data subject is exercising their right to have their personal data erased (also known as the right to be forgotten). The right to erasure is not absolute and only applies in certain circumstances.

1. Complete steps 1 to 3 under Section 4.1.1 unless already done so.
2. If not clear, confirm with the data subject the information which they wish to have erased.
3. Confirm there is an applicable circumstance in the table under Section 2.2, Rights of the Data Subject.
4. The right to erasure will not apply if processing is necessary for one of the following reasons:
    a) To exercise the right of freedom of expression and information.
    b) To comply with a legal obligation.
    c) For the performance of a task carried out in the public interest or in the exercise of official authority.
    d) For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
    e) For the establishment, exercise or defence of legal claims.
    f) If the processing is necessary for public health purposes in the public interest (e.g., 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).
    g) If the processing is necessary for the purposes of preventative or occupational medicine (e.g., where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g., a health professional).
5. Confirm the data subject has been identified correctly.
6. Delete the personal data in scope.

7. Inform any third parties or data processors who have a copy of the information of the need for deletion and request conformation this action has been completed.

8. Assess the possibility of erasure of the data from backup systems. If possible, complete the action, if not possible inform the data subject of the fact, the likely retention, i.e., before overwriting or destruction of media, and list the steps we are taking to put the backup data 'beyond use'.

9. Provide confirmation to the data subject of the actions taken, with reference to Section 3.3.1 above, on the changes made, together with confirmation of the processing activities and a copy of the relevant privacy notice.

10. Complete the relevant fields in the Rights Request log ensuring only the request is listed and not the personal data deleted.

### 4.1.4 Right to Restrict Processing of Personal Data

The data subject is exercising the right to request us to restrict how we process their data. The right to restriction is not absolute and only applies in certain circumstances.

1. Complete steps 1 to 3 under Section 4.1.1 unless already done so.

2. If not clear, confirm with the data subject the information which they wish to restrict.

3. Confirm there is an applicable circumstance in the table under Section 2.2, Rights of the Data Subject.

4. Advise the data subject they have the right to request restriction of the processing of their personal data while we are dealing with their request; however, if we believe we have a compelling reason for not doing so we will inform them of this decision and the reason(s) for it. Otherwise as a matter of good practice, we will restrict the processing of the personal data in question while we are confirming their request, whether or not the data subject has exercised this right.

5. As the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data, we will identify the most appropriate method of restriction for the type of processing we are carrying out.

6. Confirm the data subject has been identified correctly.

7. Restrict processing of the data using the chosen method, e.g., temporarily moving the data to another processing system or making the data unavailable to users.

8. Inform any third parties or data processors who have a copy of the information of the need to restrict processing and confirm they have the means to do so.

9. Assess the possibility of restriction of the data from backup systems. If possible, complete the action, if not possible inform the data subject of the fact, the likely period this could take place, i.e., before overwriting of media, and list the steps we are taking to ensure their data cannot be processed in such circumstances.

10. Provide confirmation to the data subject of the actions taken, with reference to Section 3.3.1 above, on the changes made, together with confirmation of the processing activities and a copy of the relevant privacy notice.

11. Complete the relevant fields in the Rights Request log.

12. A restriction is likely to be temporary, e.g., when the data subject has disputed the accuracy of the personal data and you are investigating this, or they have objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the data subject. The Director of organisational Services must diarise the need for follow up action. Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the data subject, you may decide to lift the restriction. However, if you do so, you must inform the data subject before you lift the restriction.

13. If the restriction is to be lifted, after informing the data subject you must also inform any third parties or data processors who have a copy of the information that the processing restriction has been lifted.

**14.** Update the relevant fields in the Rights Request log.

### 4.1.5 Right to Object to Processing of Personal Data

The data subject is exercising their right to object to the processing of their data. The right to objection is not absolute and only applies in certain circumstances.

1. Complete steps 1 to 3 under Section 4.1.1 unless already done so.

2. If not clear, confirm with the data subject the information which they are objecting to being processed.

3. Confirm there is an applicable circumstance in the table under Section 2.2, Rights of the Data Subject.

4. Advise the data subject they have the right to request restriction of the processing of their personal data while we are dealing with their request; however, if we believe we have a compelling reason for not doing so we will inform them of this decision and the reason(s) for it. Otherwise as a matter of good practice, we will restrict the

processing of the personal data in question while we are confirming their request, whether or not the data subject has exercised this right (refer to Section 4.1.4.)

5. As the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data, we will identify the most appropriate method of restriction for the type of processing we are carrying out.

6. Confirm the data subject has been identified correctly.

7. To comply with the objection a decision must be made on whether it is necessary to continue restricting processing of the data (e.g., where the data is used for other processing purposes) using the chosen method, e.g., moving the data to another processing system or making the data unavailable to users, or to erase the personal data (see Section 4.1.3).

8. Whichever decision is made, inform any third parties or data processors who have a copy of the information of the need to restrict processing or erase the data and confirm they have the means to do so and have complied.

9. Assess the possibility of restriction or erasure of the data from backup systems. If possible, complete the action, if not possible inform the data subject of the fact, the likely period this could take place, i.e., before destruction or overwriting of media, and list the steps we are taking to ensure their data cannot be processed in such circumstances.

10. Provide confirmation to the data subject of the actions taken, with reference to Section 3.3.1 above, on the changes made, together with confirmation of the processing activities and a copy of the relevant privacy notice.

11. Complete the relevant fields in the Rights Request log.

# 5 Exemptions

In certain instances, a subject access request can be denied in whole or in part. The following are valid reasons:

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 public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security

f) The protection of judicial independence and judicial proceedings

g) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

h) A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g)

i) The protection of the data subject or the rights and freedoms of others, including where others have provided a confidential reference

j) The enforcement of civil law claims

Overall, an individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, the Director of Organisational Services will establish whether the information requested falls within the definition of personal data and record any applicable exemptions.

# 6 Sanctions and Repercussions

The rights of data subjects are at the heart of the GDPR and should be considered of paramount importance over the desires of the organisation. The Rights Request Procedure is the method by which these rights are exercised.

Failure to respond correctly to a DSRR could expose Hanover to fines or other sanctions by the ICO or through legal action, and the reputational damage we would suffer, especially given we are a company who prides itself on the data protection advice we give others, could seriously impact our ability to do business.

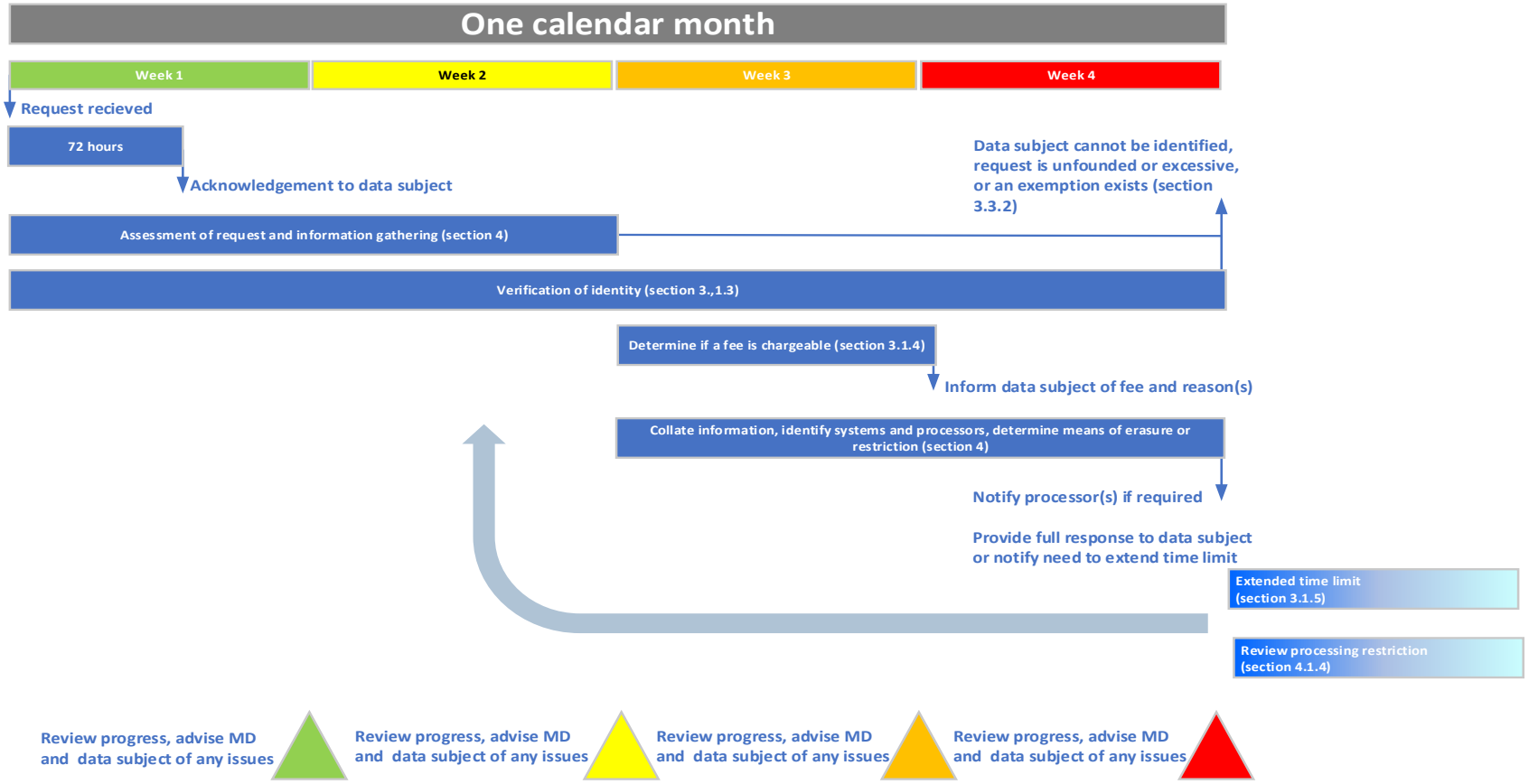
Therefore, to avoid such a situation it is imperative we respond correctly to any DSRR; do not under any circumstances:

- Ignore a request, even if it is not clear or arrives via an unexpected channel
- Keep the data subject in the dark as to what progress we are making; by being open and transparent we demonstrate our commitment to upholding their rights
- Attempt to subvert or change either the request or the response we provide

- Fail to assist the Director of Organisational Services or other management with responding to a request in a timely and correct manner

# 7 Planning and Deadlines

This diagram should be used to track activities and ensure deadlines are met.



# 8 Document Control

This policy was approved by a Director and is issued on a version-controlled basis

| CHANGE HISTORY RECORD | | | |
|---|---|---|---|
| VERSION NO. | REASON FOR CHANGE | APPROVAL | DATE OF ISSUE |
| 1 | Document creation | [APPROVER] | [DATE] |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |