

DATA PROTECTION COMPLAINTS PROCEDURE



Contents

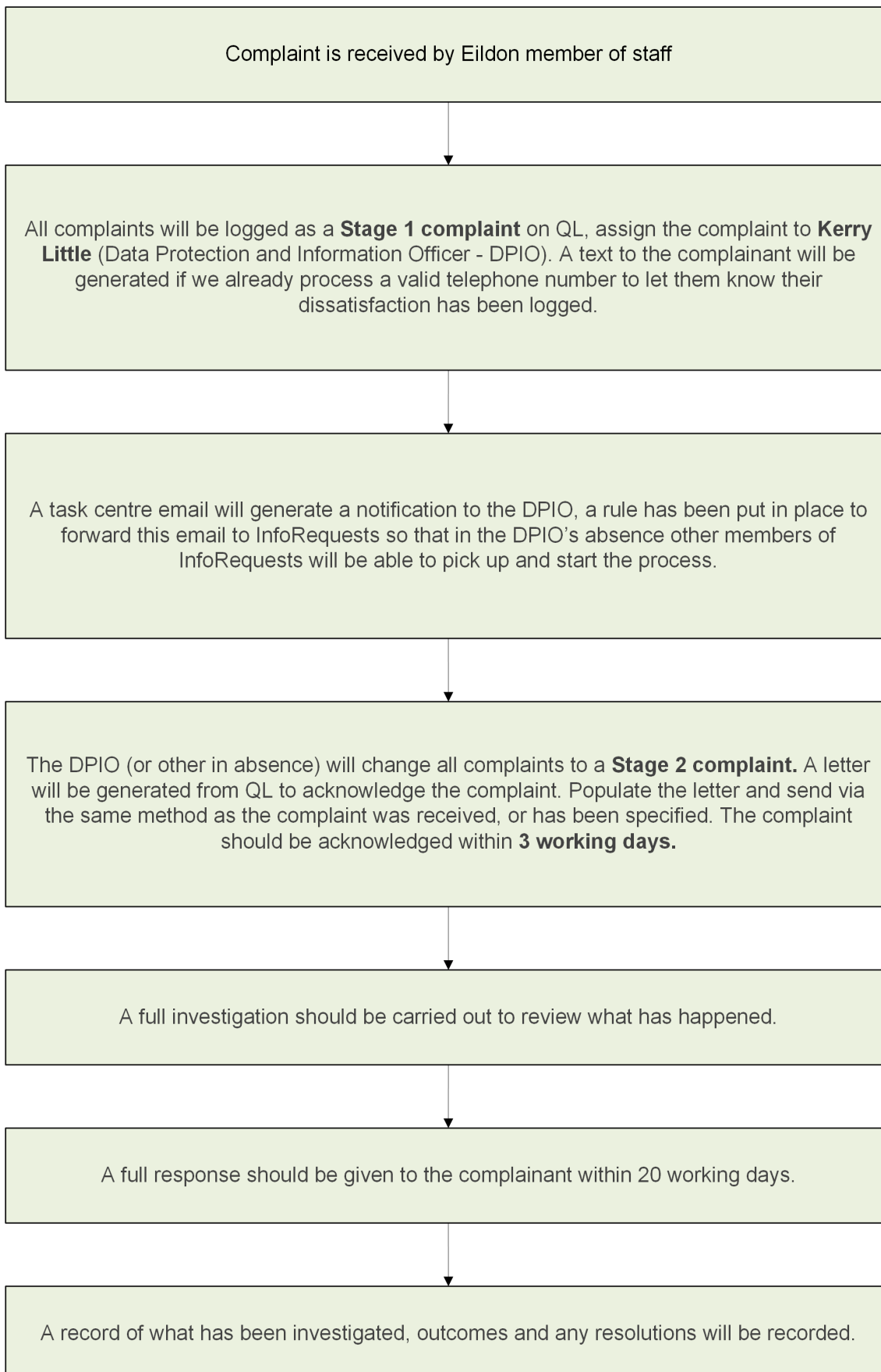
Introduction	1
1. Process	2
2. Who can make complaints	3
3. How individuals can make complaints	3
4. The investigation	4
5. What we need to record	4
6. After the investigation	4
7. Review the lessons learned.....	5
8. Contacting the ICO.....	5
9. Review of Procedure.....	5
Appendix 1 - Examples	6

Procedure Reference	
Lead Officer:	Director of Business Support
Nominated Officer:	Data Protection and Information Officer
Policy/Strategy/Framework it relates to:	Data Protection Policy
Aim of Procedure:	Complaints procedure for data protection complaints

Introduction

This procedure sets out how Eildon will handle complaints relating to the collection, use, storage and sharing of data subjects' personal data. We are committed to protecting individuals' rights and ensuring compliance with applicable data protection legislations. It seeks to resolve customer dissatisfaction as close as possible to the point of service delivery and to conduct thorough, impartial, and fair investigations of customer complaints so that, where appropriate, we can make evidence-based decisions on the facts of the case.

1. Process



2. Who can make complaints

A data protection complaint can be received from anyone who is unhappy with how we have handled their personal information. For example, they may come from someone who:

- Is unhappy with how we have responded to their subject access request (SAR), or other data subject rights request;
- Have been impacted by a data breach, regardless of whether it is reportable to the Information Commissioners Office (ICO) or not; or
- Are unhappy about the way we have used their personal information (e.g. where we have stored it, how long we have retained it, or the accuracy of the data held)

Further examples of complaints and data subject rights can be found in appendix 1.

Data protection complaints can be received from anyone that we process personal data about, this can include but is not limited to customers, applicants, and employees.

3. How individuals can make complaints

Complaints can be received via:

- The online 'contact us' form: <https://www.eildon.org.uk/contact-us/>
- By post: Data Protection and Information Officer, The Weaving Shed, Ettrick Mill, Dunsdale Road, Selkirk TD7 5EB
- By email: Inforequests@eildon.org.uk
- Over the phone
- In person
- Via Social media – however, responses will not be sent via social media and an alternative contact method should be obtained

Complaints should include:

- Individuals name and contact details;
- Details of data protection concern; and
- Any relevant dates, documents, or evidence

Verifying the authority of people making complaints on behalf of other people

Someone may make a complaint on behalf of another person (e.g. family member, solicitor etc.) In this instance we must check that they are authorised to act on the other person's behalf. The proof we will require will depend on the circumstances, but some examples are:

- An appropriate power of attorney; or
- A signed letter of authority from the person they are acting on behalf of.

If we are unsure whether a letter of authority is valid, we could consider contacting the complainant about our concerns. If we have no evidence that a third party is authorised to act on someone's behalf, we must not investigate until we receive the appropriate authority.

4. The investigation

Investigations into the complaint must happen without undue delay. Appropriate levels of enquiries should be made, and we must be able to justify why we have handled the complaint in the way that we have.

Information that we gather should include:

- Looking at all relevant facts thoroughly, fairly and accurately;
- Speaking to relevant members of staff;
- Comparing the information from the complaint to the information we hold; and
- Checking we have upheld our own terms, policies, and standards.

If we are unsure what the complaint is about, the DPIO will clarify the issue with the complainant as soon as possible. We can also clarify with the complainant what outcome they are looking for.

We must keep the complainant updated on any progress that we make, without undue delay.

5. What we need to record

We should keep a record of:

- The date complaint was received (QL record);
- Our acknowledgement;
- Any relevant conversations and documents;
- The outcome of the complaints; and
- Any actions we have taken as a result of the investigation.

Complaint records that relate to our customers or employees will be kept for the same duration of time as the tenancy or employee file; this is 5 years from tenancy or employment end date. Non tenant complaints will be kept for 2 years from the date the complaint has been closed.

6. After the investigation

Once we have completed the investigation, we must let the complainant know the outcome, without undue delay. We must be able to justify why we handled a complaint the way we have.

We should explain clearly to the complainant what we have done to resolve their data protection complaint and, where appropriate any actions we have taken as a result. This

should include enough information to help the complainant understand how we have reached the conclusion.

If the complainant is unhappy with the outcome of their complaint, we should let them know that they have the right to complain to the ICO and provide the complaint with the ICO contact details.

7. Review the lessons learned

Once we have provided the complainant with a response, we should review what has happened and consider if there is anything that we can learn or improve on to prevent future complaints. Recording this helps us identify any trends or areas to improve on. Any lessons learned that are deemed critical will be reported immediately to the Executive Team, otherwise the lessons learned will be reported quarterly in the quarter round up.

8. Contacting the ICO

If an individual is not satisfied with our response to their complaint, they have the right to contact the Information Commissioner's Office (ICO):

Website: <https://ico.org.uk/make-a-complaint/>

Telephone: 0303 123 1113

9. Review of Procedure

The Data Protection and Information Officer will ensure this procedure is reviewed every three years or earlier if there are any changes to the legislation.

Appendix 1 - Examples

Data Protection Complaint Examples:

- **‘Eildon hasn’t responded to my Subject Access Request’** – not happy with the information received in response to their SAR or not received any response from a SAR.
- **‘You sent an email to the wrong person, and it contained my personal information in it’** - not keeping information secure; /has disclosed information about you.
- **‘I asked you to update my email address 6 months ago and you haven’t’** - holding inaccurate information about you.
- **‘I asked you to delete my housing application in July’** keeping information longer than is necessary.
- **‘You told me you only needed my email address for X, why is it now being used for Y’** - collected information for one reason and is using it for something else: or
- has not upheld any of the [data protection rights](#).

Data Rights:

- **Right to be informed** - Individuals have the right to be informed about the collection and use of their personal data.
- **Right of access** - Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- **Right to rectification** - The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- **Right to erasure** - The UK GDPR introduces a right for individuals to have personal data erased.
- **Right to restrict processing** - Individuals have the right to request the restriction or suppression of their personal data.
- **Right to data portability** - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- **Right to object** - The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- **Rights related to automated decision-making including profiling** - The UK GDPR has provisions on:
 - automated individual decision-making (making a decision solely by automated means without any human involvement); and
 - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.