Data Protection Complaints Procedure

Version:	1
Approval authority:	NWT Group Strategic Leadership Team
Date 1st approved:	
Review due date:	
Authored by:	Clare Starr, Operations and Data Manager

Contents

1. Scope

It is a legal requirement to have a procedure in place to deal with data protection complaints, this requirement was brought in by the Information Commissioner's Office.

This procedure outlines The Trust's obligations and processes in relation to a data subjects' right to make a data protection complaint about the way we've handled personal data. Personal data is data that can identify a person. All personal data processed by NWT Group is within the scope of this procedure.

Personal data may include photos, videos, ANPR, dashcam footage and CCTV, as well as digital and paper documents.

It includes data that relates to a person even if it doesn't name them, including pseudonymised data where the name has been replaced with a code/number.

2. The legal requirement

Data protection law says you **must**:

- give people a way of making data protection complaints to you;
- acknowledge receipt of complaints within 30 days of receiving them;
- without undue delay, take appropriate steps to respond to complaints, including making appropriate enquiries, and keep people informed; and
- without undue delay, tell people the outcome of their complaints.

3. What is a data protection complaint?

Examples of complaints may include:

- how we've profiled them;
- invisible processing where we've processed their data and not informed them within a month;
- the way we've responded to their subject access request (SAR), or other rights request;
- how long we're keeping personal information;
- the security measures we've used to store their information (e.g. someone who has been impacted by a data breach (such as sharing their personal data with an unauthorised person), regardless of whether it was reportable); or
- how we've collected or used their personal information (e.g. where we've stored it, how long we've kept it for, or its accuracy).

4. Responsibilities

The Data Protection Officer (DPO) is responsible for this procedure and compliance with legal requirements.

Data owners and key contacts will work with The Trust's Business Support Team and the Data Protection Officer to investigate and resolve the complaint without undue delay.

The Trust's Business Support Team will log the details and save all documents. They will acknowledge the complaint without undue delay and within the 30-day period. They will monitor the time taken to complete the response and send timely reminders to those investigating the complaint.

5. Managing a complaint

The complaint can be made verbally or in writing. This includes phone calls, emails, letters, face-to-face, social media and WhatsApp messages.

Complaints from a child must be copied to the Safeguarding Lead for advice. Children have the right to complain, especially where the data was collected under the consent of an adult or guardian. We will always prioritise the child's rights and wellbeing.

Acknowledgement

You **must** acknowledge receipt of the complaint without undue delay and **within 30 days**.

- The 30 days start the day after you receive the complaint. It doesn't matter if this day falls on a weekend or a public holiday.
- If the last day to acknowledge the complaint falls on a weekend or public holiday, you have until the next working day to provide an acknowledgement.

As part of this acknowledgement:

- summarise the complaint back to the complainant, so they know you've understood the issue;
- ask them their preferred contact method for receiving updates and obtain contact details;
- provide a reference number;
- confirm that someone will be in touch to provide updates;
- do let them know if there are likely to be delays such as needing to contact a third party as part of the investigation
- follow this up in writing (if you've acknowledged it verbally)
- ask for any clarification or identification in the acknowledgment if necessary (see below).

Clarification

If you're not sure whether someone is making a data protection complaint, you **should** ask them to clarify.

If you need more information from the person, send them a data protection complaint form to complete. Note that they don't have to complete the form, but it would help to gather the relevant information. This might include asking how they have engaged with The Trust. E.g. staff, volunteer, supporter.

Identification

Complainant details can be confirmed using the Trust data systems such as the CRM or VMS. On occasion it may be necessary to request further proof of identity, this request will be made by the Trust's Business Support Team and will be made at the earliest opportunity. If adequate identification is not received within one month, the complaint will be closed.

Proof of identification would commonly be a passport, driving licence or another official photograph identification card. Details of the identification document will be recorded, along with who verified the document and the date. Only the minimum amount of data necessary for the purpose of identifying the person will be retained, it is not necessary to keep a copy of the document.

Proof of address can be found in the Trust's data systems, by sending documents to their listed address or ask for a copy of a recent bank statement or utility bill.

Someone may make a complaint on behalf of another person (e.g. a family member, solicitor, child advocacy service, or other relevant not-for-profit organisation). If so, you **must** check they're authorised to act on the other person's behalf. The form of evidence you may need depends 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;
- proof of parental/carer responsibility for a child aged over 12.

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

6. The investigation

The Business Support team will email all relevant team or system contacts likely to be required to take part in the investigation.

The data owner(s) or DPO will nominate someone to lead the investigation and draft the reply. The investigator(s) may also have to involve third parties as necessary. E.g. if the complaint involves a contract, another Trust or a third-party platform. Only share the minimum of personal data with a third party to allow them to investigate and respond.

Searches may be needed of emails, systems, paper records, photos or CCTV.

7. The conclusion

The relevant data owner(s) or DPO to nominate one person to send the response and Cc the Trust's Business Support Team.

The Trust's Business Support Team will monitor the time taken to complete the response and send timely reminders to those investigating the complaint, but they are not responsible for the complaint being dealt with 'without undue delay'. The relevant data owner(s) must be prepared to defend any delay to the ICO.

If the complainant is not happy with the response, contact your Data Protection Lead and consider what else could be done, has the Trust taken all reasonable actions and explained the response as clearly as possible?

If the Data Protection Lead is satisfied that procedures, actions and the response could be defended to the ICO, then contact with the complainant must be made and suggest they contact the ICO. The Trust will provide all documents and related information to the ICO as requested.

8. Approval and Sign-Off

This Policy has been reviewed and approved by senior leadership. It reflects NWT Group's commitment to protecting its information assets and maintaining compliance with applicable legal and regulatory requirements.

All employees, contractors and relevant third parties are required to comply with this policy and the associated procedures. The policy will be communicated to all relevant stakeholders and made available through internal systems.

9. Change Log

Date (Month/Year)	
Date change takes effect:	
Section(s) changed:	
Updated Text:	