Brook Medical Centre

Data Protection Complaints Policy

Document History

Document Reference:	…
Document Purpose:	This Policy provides advice to practices in regard to the new Data Protection Complaints process introduced by the DUAA.
Date Approved:	4 June 2026
Version Number:	1.0
Status:	FINAL
Next Revision Due:	June 2027
Developed by:	Paul Couldrey – DPO
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2025/26

Table of Contents

Introduction

The Introduction of the Data Use and Access Act 2025 has created a new, mandatory statutory complaints-handling framework for GP Practices which takes effect on June 19th, 2026. This gives individuals the right to complain directly to a data controller, (the practice) and requires Brook Medical Centre to acknowledge complaints within 30 days and respond without undue delay.

Mandatory Data Protection Complaints Process

Under this new framework, patients are expected to seek resolution directly with the practice before escalating issues to the Information Commissioner's Office (ICO).

Brook Medical Centre meets the following statutory obligations:

- Providing patients with a straightforward way to raise a data protection complaint, this contact ddicb.bmc@nhs.net is also published in the practice's Privacy Notice.
- Officially acknowledging receipt of the complaint within 30 days.
- Informing the practice DPO of the complaint and seeking advice
- Investigating and responding to the complainant "without undue delay," keeping them updated on the progress.
- Formally notifying the individual of the outcome of the investigation.

What are data protection complaints?

The ICO defines a Data Protection complaint as “If someone considers that you've infringed data protection legislation because of the way you've handled their personal information (or the personal information of someone they're acting on behalf of).

To complain, patients don’t have to use legal terms or quote sections of the legislation.

For example, people may submit complaints about:

- the way you’ve responded to their subject access request (SAR), or other rights request.
- the security measures you’ve used to store their information (e.g. someone who has been impacted by a data breach, regardless of whether it’s reportable to us); or
- how you’ve collected or used their personal information (e.g. where you’ve stored it, how long you’ve kept it for, or its accuracy).

Sometimes people may complain about your service or other matters, whilst also exercising their data protection rights. This doesn’t count as a data protection complaint. For example:

- a patient may raise a treatment complaint, and request copies of their personal information; or
- a patient may complain about a staff attitude and request that you delete their information.

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

What do we do when we receive a complaint?

You **must** acknowledge receipt of the complaint within 30 days. What information you include is up to you, but the important thing is that you confirm you've received it and you'll investigate the issues raised.

You can acknowledge a complaint in different ways, for example:

- If you receive a complaint electronically (eg through email or live chat), you **could** use an automatic response, such as auto-acknowledgement emails. If you receive it through social media, you **should** ask for an alternative contact method as this is generally not a secure way to send personal information.
- If you receive a complaint in writing (eg by post), you **could** send an acknowledgement letter.
- If you receive a complaint verbally (eg over the phone or face-to-face), you **could** acknowledge this verbally. For example, you **could**:
    - 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, if you use them.
    - confirm that someone will be in touch to provide updates; and
    - follow this up in writing (even if you've acknowledged it verbally).

For all Data Protection complaints, regardless of how you receive them, you must store a copy of your acknowledgement to show you've met the obligations within the 30-day timeframe.

There are two important things to know about the timeframe:

- 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. The 30 days still start on this day.
- 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.

-

Example

You receive a data protection complaint on Thursday 5 June. The 30 days don't begin until the start of Friday 6 June. This means 30 days end at the end of Saturday 5 July. However, as this falls on a weekend, you have until the end of Monday 7 July to acknowledge the complaint.

If you have staff absence for certain periods of the year (eg school holidays or sickness), you **must** plan for acknowledging data protection complaints during these times.

Investigating the complaint

You **should** start by gathering as much information as you need, including:

- look at all the relevant facts thoroughly, fairly and accurately.
- speak to relevant members of staff.
- compare the information from the complaint with the information you hold; and
- check you've upheld NHS and Practice terms, policies and standards.

If you aren't sure what the complaint is about, you **should** ask the person making it for more information as quickly as possible. This helps you identify which enquiries you need to make. You **could** also ask what outcome they're looking for.

Inform the DPO

You can take advice and guidance from your DPO and should inform them of any Data Protection Complaint received immediately to ensure your responses are appropriate, the practice DPO is:

PCIG Consulting Limited

Email: Info@PCDC.org.uk

Complaints from children

Children have the same rights over their personal information as adults. However, children merit specific protection as they may be less aware of:

- the risks and consequences of the processing; and
- their rights when you process their personal information.

If Brook Medical Centre receives complaints from children, the practice **should** respond in plain, clear language they can understand.

Brook Medical Centre **must** assess the competence of the child to understand and exercise their rights. In most cases, if you've already recently assessed the child's competence as part of an initial information rights request, you won't need to do this again

Complaints made on behalf of others

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.

Confirm the complainant's identity

If you have any doubts about the complainant's identity, you may need to ask them for proof of ID before you respond. You **should** make sure you ask for it at the earliest opportunity. If you have sufficient information to be satisfied about the requester's identity, you **must not** request more information.

Investigate the complaint without undue delay

You **must** make enquiries into the complaint without undue delay. In other words, without an unjustifiable or excessive delay.

Your obligation to investigate begins when you receive the complaint, not after the 30-day acknowledgement period.

What is unjustifiable or excessive always depends on the circumstances and varies from one complaint to another and from one organisation to another. The important thing is to consider all the circumstances of the complaint, not to apply a set period as a blanket approach.

The time it takes you to investigate is likely to be impacted by:

- the complexity of the complaint.
- the scale of the issue (eg whether it's a singular complaint about a recent issue, or a complaint about several issues over a longer time); and
- any harm that the complainant is suffering because of the unresolved issue.

You **must** make an appropriate level of enquiries based on the circumstances of each complaint and be able to justify why you handled a complaint in the way you did. You're not required to take steps that would be unreasonable or disproportionate, which will always depend on the circumstances.

Keep the patient informed

You **must** keep the person making the complaint updated on the progress of the investigation without undue delay.

Record your actions

You **should** keep a record of:

- the date you received the data protection complaint;
- your acknowledgement;
- any relevant conversations and documents;
- the outcome of the complaint; and
- any actions you took as a result of your investigation.

This provides evidence of what you've done.

You **must not** keep personal information for longer than you need it.

Actions Following the investigation

Having completed your investigation, you **must** let the complainant know the outcome without an unjustifiable or excessive delay.

You may be able to investigate the complaint and provide an outcome within 30 days. In these instances, you're not required to provide an acknowledgement and outcome separately.

How you communicate with the complainant at all stages of the process is up to you, subject to any relevant equality legislation requirements. For example, you may be able to resolve more straightforward complaints quickly over the phone, provided you've verified the person's identity.

You **should** clearly explain what you've done to resolve their data protection complaint and, where appropriate, any actions you've taken as a result. If you think that you've complied with data protection law, explain this in detail to the complainant. Provide enough information to help the complainant understand how you've reached your conclusion. It can be useful to itemise the complaint areas in a bullet point list, responding to each point and providing appropriate evidence, where possible.

If the complainant is unhappy with the outcome, you could provide more detail or clarify your decision. You could consider having a review process for complainants that remain unhappy with the outcome of their complaints.

It's also good practice to let them know they have the right to complain to the ICO and provide contact details.

Patients can still complain to the ICO during or after the investigation, even if they have not received the outcome yet, unlike the general NHS Complaints Process.

Review the lessons learned

Once you've provided an outcome, {practice Name] will review the compliant and identify any lessons learnt or improvements that could be made to prevent future complaints.

Equality and Diversity

The Practice aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Practice must have due regard to the Public-Sector Equality Duty (PSED). This applies to all the activities for which the Practice is responsible, including policy development, review and implementation.

Due Regard

This policy has been reviewed in relation to having due regard to the Public-Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

Policy Review and Monitoring

The Practice Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.

This policy will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.