Scottish Courts and Tribunals Service

Data Protection Complaints Policy

Publication Date:	**15 June 2026**
Version:	0.3
Review Date:	Every two years

Version Control

Date	Version	Author Initials	Description of Change
12/05/2026	V.01	LJ	Created and distrubuted for comment and review to IGCT
20/05/2026	V0.2	LJ	Updated with IGCT comments – circulated to TSBU, HR and OPG for review
15/06/2026	V0.3	LJ	Published

Scottish Courts and Tribunals Service

Purpose

This policy explains how the Scottish Courts and Tribunal Services (SCTS) handle complaints about the way we process personal information, to ensure we meet our legal obligations and resolve issues fairly and promptly. It adopts the guidelines set out by the Information Commissioner's Office (ICO) in relation to data protection complaints and aims to review and resolve matters prior to the involvement of the ICO.

Scope

This policy applies to:

- All personal information processed by SCTS in its role as a data controller.
- Complaints from any individual (including someone acting on another's behalf where properly authorised).
- Complaints relating to processing under UK GDPR and (where applicable) processing under Part 3 DPA 2018 (law enforcement processing).

Policy Statement

We will maintain and operate an internal process for handling data protection complaint.

We will:

- Provide a clear way for people to complain to us directly.
- Acknowledge complaints within 30 days.
- Investigate and respond without undue delay; making appropriate enquiries and keeping people informed.
- Provide the outcome without undue delay.

What is a 'data protection complaint'

A data protection complaint is where someone considers we have infringed data protection law because of how we handled their personal information (or information of someone they represent).

Complainants do not need to use legal terminology or cite legislation for it to be treated as a complaint.

Examples include complaints about:

- How we handled a subject access request or other rights request.
- Security measures used to protect personal information (including where someone is affected by a breach, whether or not it is reportable to the ICO).
- How we collected, used, stored, retained, or kept information accurate.

Not all “complaints” are data protection complaints. For example, a service complaint that also includes a request to delete information, or an employee grievance with a request for copies of data, is not necessarily a data protection complaint.
If unclear, we will ask the individual to clarify whether they intend to make a data protection complaint.

Where a data protection complaint forms part of a complaint about a wider issue, we will respond to the data complaint element as soon as we can. In some circumstances, it may not be possible to provide an outcome until the wider issues are investigated.

How to make a complaint

People can complain using any channel. We will accept complaints however they are received, including where the complaint is made to any member of staff or via other organisational routes.

We offer the following routes (preferred but not mandatory):

- Email: DPO@scotcourts.gov.uk
- Post: Scottish Courts and Tribunals Service, O1 Spur, Saughton House, Broomhouse Drive, Edinburgh, EH11 3XD
- Online form Data protection | Scottish Courts and Tribunals Service

Social media

If a complaint is received via social media, we will usually ask for an alternative contact method because social media is generally not a secure way to exchange personal information.

Telling people about the right to complain

We will tell people they can complain:

- At the point we collect their personal information (e.g. in our privacy notice and individual rights guidance), using clear and plain language.

- When responding to a subject access request (and other relevant rights interactions, as applicable).

Complaint handling process

Recording and triage

On receipt, we will:

- Log the complaint, date received.
- Identify whether it is a data protection complaint (and seek clarification if needed).
- Identify any immediate risks (e.g. ongoing harm that should be prioritised).

Identity checks

If we have doubts about the complainant's identity, we may ask for proof of ID and will do so at the earliest opportunity.

If we do, we will ask you to provide us with proof of your identity and of your address We ask if required that you supply us with a photocopy or scanned image (do not send the originals) of the following:

1) Proof of Identity

Example include: passport, photo driver's license, national identity card, birth certificate.

2) Proof of Address

Examples include: utility bill, bank statement, credit card statement (no more than 3 months old);

If we are not satisfied you are who you claim to be, we reserve the right to refuse to investigate your complaint.

If we already have sufficient information to be satisfied about identity, we will not request additional information.

Complaints made on behalf of someone else

Where someone complains on behalf of another person, we may need to verify they are authorised to act on behalf of the complainant.

If we do, we will ask for proof that the individual making the complaint is authorised to do so, this may include (e.g. power of attorney or signed authority). We will also require proof of the complainant's identity and that of the person making the complaint on behalf of the complainant, examples of valid forms of ID are provided above.

We may contact the other person to ensure the authority is valid.
We will not investigate until proof of appropriate authority is provided, if requested.

Acknowledgement

We will acknowledge receipt of the complaint within 30 days.

The 30 days start the day after the complaint is received, if the last day falls on a weekend/public holiday, acknowledgement is due by the next working day.

If we have requested proof of identity, the clock will be paused and will restart once proof of identity is received.

We will keep a record of the acknowledgement as evidence of compliance.

Investigation

We will make enquiries without undue delay; the obligation starts when we receive the complaint, not after the acknowledgement period.

We will take an appropriate and proportionate approach, considering factors such as complexity, scale, and any harm being suffered.
We will typically:

- Gather and review relevant facts fairly and accurately.
- Speak to relevant staff/teams.
- Compare the complaint to the information we hold
- Check that SCTS policies and standards have been upheld.

If we use internal guideline timescales, we will ensure these do not create unjustifiable delay and will conclude sooner where possible.

Keeping the complainant informed

We will provide the complainant with an acknowledgement within 30 calendar days. This will include a timescale for response based on initial investigation.

If after further investigation we require further time, we will provide a further update no later than the original expected timescale for responding.

Outcome

After completing the investigation, we will provide the outcome without undue delay. Our response will clearly explain:

- What we found and how we reached our conclusion (with enough detail to understand our reasoning).
- What we have done to resolve the issue and any actions taken (where appropriate).

Escalation to the ICO

Individuals have the right to lodge a complaint with the Information Commissioner (ICO) if they consider processing infringes data protection law.

We will provide ICO contact details as part of the complaint response.

Record Keeping

We will keep a record of:

- Date received and how it was received.
- Acknowledgement.
- Key correspondence, conversations, and documents.
- Outcome and actions taken.

We will not keep personal information for longer than we need it.

Roles and Responsibilities

- All staff: Must recognise potential data protection complaints and route them to DPO mailbox promptly because complaints can be made through any channel.
- DPO - Complaint owner: Oversees recording, investigation, updates, and outcome.

- Business Units: Provide information and support enquiries without undue delay.

Training and awareness

We will ensure staff can recognise data protection complaints and know what to do if they receive one.

Monitoring and improvement

After outcomes are issued, we will review lessons learned and consider improvements to prevent recurrence and identify trends.

Review

This policy will be reviewed every two years or sooner if regulatory guidance or legislation changes.