

## Privacy Notice

### Processing by the First-tier Tribunal for Scotland (Tax Chamber)

#### What is being processed?

The [First-tier Tribunal for Scotland \(Tax Chamber\)](#) decides appeals against Revenue Scotland's decisions relating to devolved taxes

The amount of personal data processed by the Tax Chamber is limited to that in relation to identity, address and contact details of appellants.

#### Why are we processing this information?

Processing of tribunal case information is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" in terms of Article 6(1)(e) of the GDPR.

#### What categories of personal data are you processing?

The Tax Chamber does not process personal data in relation to any of the special categories of personal data listed in Article 9(1) of the GDPR, The only anticipated circumstance would be in a situation where a person sought a discharge of a hearing on grounds of ill-health and provided a soul and conscience doctor's letter in support. This would be retained with the case papers. Any such processing would be necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity in terms of Article 9(2)(f) of the GDPR.

#### Where do you get my personal data from?

The Tribunal may receive your data from the following sources

- You may provide your own data to the Tribunal
- Your representative(s) may provide data to the Tribunal
- Revenue Scotland
- Scottish Environmental Protection Agency

#### How, when and why does the SCTS share this personal data with others?

Hearings are usually held in public and decisions are published on the Tax Chamber's website. Plainly a decision would include the name of the appellant and the subjects of the appeal (in a LBTT case). The appellant's address might be capable of identification in certain cases. Information may be shared with Revenue Scotland and the Scottish Environmental Protection Agency if necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller in terms of Article 6(1)(e) of the GDPR.

#### Do you transfer my personal data to other countries?

No

#### How long do you keep my personal data?

We retain hard copy Tribunal case papers for as long as a case, or an appeal of that case, is in process, Electronic copies of all case papers are stored securely on our case management system and processed in line with our records management plan.

#### Do you use automated decision making or profiling? If so, how do you use my personal data to make decisions about me?

No automated decision making or profiling takes place.

## Scottish Courts and Tribunals Service

The [Scottish Courts and Tribunals Service](#) (SCTS) provides administrative support to [courts](#) and [tribunals](#) in Scotland. If you are involved in a court case or tribunal hearing, we are highly likely to process your personal data and to retain at least some of it. This processing is necessary in the public interest in order to fully support all aspects of the progression of a case through Scotland's courts and tribunals, including the defending and establishing of rights.

We also support the [Judiciary](#) and the [Office of the Public Guardian](#). Records of each court or tribunal case and/or hearing are retained and some details – for example, the sentence in a criminal case or the outcome of an adoption – will be permanently archived as a part of Scotland's [national records](#). Some personal data may be shared with other persons or organisations when required or justified by law.

You are entitled to [ask us](#) for a copy of any of your personal data that we hold and to ask about why and how your personal data is held, processed, retained and shared. You can also [challenge us](#) if you think that we are processing your personal data inappropriately or if you consider that the information held is inaccurate.

As set out in its [Information Assurance Statement](#), the SCTS is committed to ensuring all personal information is collected and processed in accordance with data protection law.

[The Data Protection Principles](#)

[General Information](#)

[What are my rights?](#)

[How does the SCTS keep information secure?](#)

## The Data Protection Principles

Article 5 of the [General Data Protection Regulation](#) (GDPR) obliges the SCTS to ensure that personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**'purpose limitation'**);
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- (d) accurate and, where necessary, kept up to date (every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay) (**'accuracy'**);
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).

Similar principles in relation to processing of personal data in criminal court cases (processing for "law enforcement purposes") are set out in sections 35 to 42 of the [Data Protection Act 2018](#).

## **General Information**

### **Marketing**

The SCTS will not share personal data with third-parties for marketing purposes.

### **Research**

The SCTS may grant research access to certain pre-approved researchers to historical case data for research purposes (e.g. sociological research on access to justice), subject to suitable protections for the privacy of those featured in the cases.

### **Consent**

The SCTS observes the Information Commissioner's Office (ICO) best practice guidance in not asking persons for [consent](#) in relation to the processing of personal data. We may ask for permission to process certain data in limited circumstances where it is completely clear that consent is entirely voluntary, for example in relation to customer satisfaction research.

### **Automated decision making or profiling**

The SCTS conducts limited [automated decision making or profiling](#). This occurs in relation to staff recruitment, attendance management and in relation to selection as a prospective juror. For further information, see the [Headquarters](#) and [Jury Service](#) sections of this Privacy Notice.

### **Website**

Information on user anonymity for use of our website is available at <http://www.scotcourts.gov.uk/meta/privacy>.

### **Data Protection by Design**

The SCTS is committed to ensuring that only personal data necessary for the specific purpose identified for the processing are processed.

### **Data Protection Officer / Data Controller**

The SCTS is a Data Controller. Its Data Protection Officer is Iain Hockenfull, Head of Information Governance and Correspondence. Please email [dpo@scotcourts.gov.uk](mailto:dpo@scotcourts.gov.uk) for further information. The postal contact is: N1 Spur, Saughton House, Broomhouse Drive, Edinburgh, EH11 3XD.

## What are my rights?

- You have the right to obtain confirmation that your data is being [processed, and to access to your personal data](#)
- You have the right to object to processing [in specific circumstances](#)
- Special rights apply in relation to the processing of personal data in respect of [children](#)

### **Right of access**

You have the **right to access personal data** that we hold. This right will normally operate so as to provide you with your personal data within one month. There is no fee, but we will ask you to prove your identity. There are some circumstances in which we may require more time to locate your information or where material cannot be provided, for example where disclosure might have an adverse impact upon on-going proceedings or where the personal data of other persons is also featured. In handling requests we will inform you of any such limitations placed upon the right of access and to your right to appeal to the UK Information Commissioner. More information on Subject Access Rights can be accessed [here](#).

### **Right to erasure**

You have the [right to request that we cease or limit our processing](#) of your personal data. Please note that this right is unlikely to apply where processing remains necessary in relation to the purposes for which the data were collected. For example, the SCTS is obliged by Public Records legislation to preserve records of criminal and civil court cases: it is highly unlikely that the right to erasure could be used to entirely erase those records, but you might be able to exercise it in relation to some specific processing.

### **Right to rectification**

You have the [right to request that we correct or amend our records](#) if you have reason to think that we have made a mistake in recording or processing your personal data, for example that it is inaccurate or incomplete.

*Note: these rights are unlikely to apply where personal data is being processed during the course of court or tribunal proceedings. Articles 15 (right of access by the data subject), 16 (right to rectification), 17 (right to erasure) and 18 (right to restriction of processing) of the GDPR do not apply to personal data processed by a court or tribunal acting in a judicial capacity (see paragraph 14 of Schedule 2 to the [Data Protection Act 2018](#)).*

### **How do I complain if I am not happy?**

If you are unhappy with any aspect of this privacy notice, or how your personal information is being processed, please contact the SCTS Data Protection Officer at:

[dpo@scotcourts.gov.uk](mailto:dpo@scotcourts.gov.uk)

**If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):**

#### **Information Commissioner's Office**

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Tel: 0303 123 1113

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk)

<https://ico.org.uk/global/contact-us/>

## How does the SCTS keep information secure?

The SCTS Data Security Policy sets out the security standards in place in relation to all personal data. It includes:

- Staff should not take any laptop, or removable drive or external medium, containing personal or sensitive data stored in an unencrypted medium outside secure office premises.
- Staff should not carry or take any official information, data or records outside SCTS premises unless for an authorised purpose. Staff must not carry personal or sensitive data outside SCTS premises on laptops or memory sticks without good cause, even when that data is stored in encrypted form.
- Staff must not, under any circumstances, store personal or sensitive data on the C: drive of their PC or laptop unless it is stored in an encrypted working medium, nor should they store personal or sensitive data on any unencrypted removable media such as a USB memory stick.
- Staff should ensure at all times that access to equipment and media is password protected – all passwords should be chosen carefully and disclosed to no-one else;
- Staff should consider ways to best protect sensitive information before sending on and should always limit access to those who need to use the information;
- Access to IT systems containing personal data is provided on a need to know basis, and access to information protected by a unique logon and password. Access must be used for legitimate business purposes only, and systems have an audit function to allow inappropriate access to be detected.
- Under no circumstances should staff:
  - access or attempt to access another employee's computer, computer account, laptop, blackberry, mobile, e-mail or voice mail messages, files or other data, government or private data without authorisation (e.g. as a part of a corporate security investigation); or
  - misuse information which they acquire in the course of their official duties, nor without authority disclose official information which has been communicated in confidence within SCTS or as part of the Scottish Government, or received in confidence from others.
- The SCTS has adopted the UK Government security classification scheme for protective markings signifying the level of security that should be allocated to each document.

The SCTS is an accredited member of the Public Secure Network (PSN): the secure network used by other public bodies such as the COPFS and Police Scotland to transfer sensitive data electronically.

All SCTS staff have been disclosure checked and Baseline Personal Security Standard (BPSS) checks are conducted on all SCTS staff and on contractors and agency staff. All permanent staff and non-staff must have the BPSS clearance before they are allowed to access buildings, assets or information.

Electronic court case management systems are access controlled. Restricted and relevant access is controlled by local court managers. The system is updated as cases progress through the courts.