

Judicial Office
for Scotland



IT & Information Security Guide for Judicial Office
Holders in Scotland
Protecting Information: Prevention of and Management
of Incidents

This guidance is issued by the Lord President under s.2(2)(d) of the Judiciary and Courts (Scotland) Act 2008 and s.34(1)(a) and (b) of the Tribunals (Scotland) Act 2014

28 February 2012
Version 2 - Revised 13 February 2013
Version 3 – Revised May 2015
Version 4 – Revised December 2018

1 INTRODUCTION

- 1.1 Members of the Judiciary are provided with IT services to support them in the performance of their judicial duties. For example, IT user accounts, mailboxes with email addresses and SCTS-managed equipment such as desktops, individually issued laptops and mobile phones. This guidance is drafted with all judicial office holders in mind though not all will have access to all of those services.
- 1.2 All equipment issued by SCTS incorporates security features designed to protect data which the equipment is expected to handle in the course of judicial business. For official documents bearing a security classification, this means documents marked as, up to and including, OFFICIAL-SENSITIVE. Should there be a need to process official documents bearing a higher classification, e.g. SECRET in a terrorism case, then a judicial office holder must raise this with the clerk of court who will liaise with SCTS IT Department.
- 1.3 The devices and services offered to judicial office holders have been designed to provide proportionate and reasonable protection for the individual user and the organisation.

2 YOUR RESPONSIBILITIES

2.1 Safeguarding personal and/or sensitive information

- 2.1.1 Judicial office holders have a duty to safeguard sensitive and/or personal information from unauthorised disclosure. It applies to hard copies as much as to electronically stored information. The steps that should be taken to fulfil this duty will vary with the importance and sensitivity of that information. The information held by judicial office holders on computers and in hard copy varies in its importance and in its confidentiality. At one end of the spectrum is information that is already in the public domain, such as judgments that have been issued and statutes and authorities that have been published. At the other end of the spectrum is information which, if obtained by unauthorised persons, may put identified persons or members of the public at risk; closed evidence in a suspected terrorist control order case, or personally identifiable information (PII) material about an anonymous witness who fears that disclosure of his or her identity will put him or her at risk of retribution, are examples.
- 2.1.2 In between these extremes is information that is security related or commercially sensitive, such as a draft judgment in an important intellectual property case that will affect the value of a party's publicly quoted shares, and information the disclosure of which would be embarrassing, such as a less-than-glowing reference for a person seeking appointment to judicial office or the office of Queen's Counsel. A draft judgment in a case that is not of public importance or of personal significance to the parties and contains no sensitive personal information will be something which it would be unfortunate to lose, and could cause embarrassment and reputational damage, and possibly a

duplication of work, but it would not be of the same importance as more sensitive material. It should however, be regarded as sensitive whilst in the process of being drafted; i.e. being passed to secretarial staff for typing.

- 2.1.3 This guidance applies to any material that falls within those parameters - whether it is judicial, personal, or court or tribunal files, and whether the information is held in electronic or hard copy format. The General Data Protection Regulation and the Data Protection Act 2018 (“the legislation”) have more restricted definitions of "personal data" or "special category personal data" but this guidance encompasses data falling within both definitions.

What is “personal data”?

- 2.1.4 Although this guidance applies to all types of sensitive information (whether or not it is personal data), it may be useful to give a brief explanation of how the legislation defines personal data, because particular obligations exist under the legislation in respect of that category of information.
- 2.1.5 In essence, the legislation defines personal data to mean information about an identified or identifiable living individual who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. It may include personal information relating to court and tribunal users, SCTS staff and the judiciary. It includes expressions of opinion about a person and any indication of someone’s intentions in respect of that individual.

The Judiciary and the legislation

- 2.1.6 **All judicial office holders must observe the data protection principles.** Observance of this guidance is therefore important.
- 2.1.7 This guidance gives practical and proportionate ground rules for judicial office holders. None of it is particularly new or innovative. Much of it is already done by judicial office holders as a matter of course. All judicial office holders are required to ensure the safe custody of personal data for which he or she is responsible; and personal data which a judicial office holder is processing and for which the SCTS is data controller.
- 2.1.8 The Lord President has appointed a “Data Protection Supervisory Judge” who is responsible for supervising compliance with the legislation, raising awareness of it among the judiciary and handling complaints about judicial processing. The Data Protection Supervisory Judge considers complaints received about the judicial processing of personal data.
- 2.1.9 In some circumstances an incident may be so serious that it could be dealt with under the Complaints about the Judiciary (Scotland) Rules 2017 or the Complaints about the Scottish Tribunals Rules 2018. The extent to which this guidance has been observed is likely to be a relevant consideration.

2.1.10 When working with local court or tribunal staff, staff are subject to the SCTS Data Security Policy. They may be subject to disciplinary action if they breach that policy. They should not be pressed into doing something which puts them in an impossible position.

2.1.11 The important thing is to respond speedily to any incident. The sooner this is reported, the sooner action can be taken to recover the material or mitigate the breach.

2.2 **Data Breach Incidents**

2.2.1 A data breach is defined by the legislation as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

2.2.2 The list below is not exhaustive but examples include:

- Loss of a court file, or one turning up where it should not be;
- Theft of a computer containing personal data;
- Leaving a document, computer disk or memory stick containing personal information on a train or in any non-secure environment;
- Personal data held on an electronic device is viewed, obtained or otherwise accessed by someone who has no valid reason to do so (e.g. the device is hacked or a passenger on a train sees material on a laptop);
- Sending or sharing personal data to an electronic device by an unencrypted or unsecure medium;
- The inadvertent release of personal details in an email chain or sending an email with personal data to an unintended recipient;
- The deletion or destruction of information accidentally or intentionally, when it ought to be retained.

What action to take when a breach occurs or data is missing?

2.2.3 If a judicial office holder identifies a data breach or becomes aware of a suspected data loss he or she must act quickly to protect individuals whose data may be lost/compromised. The judicial office holder must **immediately** inform:

- the Judicial Office by telephone (0131 240 6677);
- the SCTS data breach team by telephone (0131 444 3312); and
- where appropriate, the Principal Clerk or Sheriff Clerk (if, for example, a breach involves the loss of court files) or Clerk to the Tribunal so that

steps are taken to address, minimise and contain risks arising from the loss/compromise.

- 2.2.4 The judicial office holder should then send an email to both the [Judicial Office](mailto:judicialofficeforscotland@scotcourts.gov.uk)¹ mail box and the [SCTS data breach centre](mailto:databreach@scotcourts.pnn.gov.uk)² providing as much information about the loss as is available using the form in the Appendix to this guide. It is important to pass on information as quickly as possible. Please do not wait for the full facts of the case to be known or until all boxes in the form are able to be completed.
- 2.2.5 The impact of the loss will be assessed by the **Judicial Office**. **They will take the lead in responding** to it. Notification is essential because, if the breach is likely to pose a risk to the rights and freedoms of individuals whose personal data is involved in the breach, then, if the data breach concerns data within the Information Commissioner's remit, the Information Commissioner's Office must be informed within **72 hours** of the judicial office holder discovering the breach or suspected breach or becoming aware of it. If the breach concerns data which is outside the Information Commissioner's remit, notification must be given to the Data Protection Supervisory Judge within the same 72 hour period. If there is a high risk to the rights and freedoms of individuals, the data subjects will need to be told.
- 2.2.6 The judicial office holder must notify his or her senior judge locally. For the sheriff and JP courts this is the sheriff principal or, where the sheriff principal is responsible for the breach, the Lord President. For tribunals it is the chamber president or, where the chamber president is responsible for the breach, the President of the Scottish Tribunals. In the Supreme Courts it is the Lord President.
- 2.2.7 Compliance with this guidance is important. The Information Commissioner has stated that the loss of any laptop or removable media, which is not encrypted, is likely to be found to be a data breach. In certain circumstances, where the Information Commissioner has a supervisory jurisdiction, (e.g. where the judicial office holder is not processing personal data in a judicial capacity) the Information Commissioner may impose a fine, where you are the data controller, for a data breach. The Data Protection Supervisory Judge has no power to impose a fine but, as mentioned above, a data breach could be sufficiently serious as to amount to a judicial conduct issue.

What is the impact of the loss?

- 2.2.8 In assessing the impact of the loss, the Judicial Office will take into account the individual circumstances of a case. This will include the impact of the data loss on the data subject, the number of people affected by the loss, the impact on court business, the damage to the reputation of the Judiciary, whether or not there is (or is likely to be) media interest and if an individual's personal safety is at risk.


¹ judicialofficeforscotland@scotcourts.gov.uk

² databreach@scotcourts.pnn.gov.uk

2.2.9 The Judicial Office will review all data loss incidents reported to them on a quarterly basis so that any trends or control weaknesses can be identified.

3 GENERAL GUIDANCE (Judicial office holders with SCTS equipment)

3.1 Locking devices

3.1.1 Leaving a computer on and unlocked when leaving chambers means that anyone who comes in may access the same information that the judicial office holder has access to. This includes locally stored files, the SCTS network, personal mailbox and, potentially, case management systems. If a laptop/computer requires to be left unattended the electronic lock should be applied. This is done by pressing the Windows key, , and L (for Lock). This is particularly important if working in a public area or outwith an SCTS building. The computer is unlocked by inputting the judicial office holder's username and password. For longer periods the judicial office holder should log off completely.

3.1.2 If leaving a laptop unattended for any period of time it should be secured to the desk/bench using a lock. Locks are available from the IT unit [deployment support team](#)³. Alternatively it should be locked away in a secure drawer or cabinet. These standard precautions minimise the opportunities for theft, which not only involves a breach of data security but cost and disruption.

3.2 Saving Files

3.2.1 All the SCTS-managed laptops which are issued to judicial office holders have hard disks which are encrypted. Encryption means that the data on disk is stored in such a way as to render it unreadable without the correct key (password). Encryption ensures that the data on the disk cannot be accessed by removing the disk and trying to read the data directly. If the laptop is stolen, so long as the system was locked or logged off, the risk of the data being compromised is acceptably low. With the advent of Windows 10, encryption will be included as standard on desktops as well as laptops. A similar encryption standard is in place on SCTS issued smart phones.

3.2.2 All judicial office holders who have an IT account (Judges, Sheriffs, Justices of the Peace but not Tribunals Members) have a personal (P:/) drive, which is a part of the central data storage on the SCTS network. The P:/ drive is only accessible by the individual judicial office holder and a small number of IT administrators who may only access it when there is a network security issue or to deal with an IT issue raised by the judicial office holder. The P:/ drive is backed up overnight along with all the other network drives. The P:/ drive is accessible from SCTS desktops and laptops when connected through a wired or wireless connection to the SCTS network. The P:/ drive is also accessible when connected to the SCTS network through the SCTS VPN (Virtual Private Network), i.e. via the Internet away from the SCTS estate. For the reasons mentioned, the P:/ drive is the preferred location for judicial office holders to store their files.

³ dst@scotcourts.gov.uk

- 3.2.3 Judicial office holders who have been issued with laptops (Judges and Sheriffs) have the option to store files locally on the laptop's C:/ drive. The C:/ drive is encrypted but it is **NOT** backed up. There will be no backup or copy unless the judicial office holder has made one. Loss of, or serious damage to, a laptop or failure of the laptop or disk will result in the loss of the data stored on it. It is recommended that judicial office holders move files which they are actively working on to the C:/ drive only when they wish to work on them from outside an SCTS building.
- 3.2.4 Justices of the Peace and Tribunal Members who receive sensitive data to their CJSM email addresses and store the information locally, do so at their own risk. See the section [Using Non-SCTS Equipment](#) below.
- 3.2.5 Judicial office holders may wish to work on non-SCTS issued devices and to transfer information to them using a USB drive. Removal of data from the SCTS-managed network and SCTS devices takes it beyond SCTS protection and is done at the judicial office holder's own risk. As a minimum, SCTS recommends that data is saved on encrypted USB drives. They can be requested from IT Unit [deployment support team](#)⁴. The password for an encrypted USB drive must not be stored with the drive. Data cannot be recovered in the event of a hardware failure or if the password is forgotten. Any files stored on an encrypted USB drive should also be saved to a network drive to ensure there is a backup copy.
- 3.2.6 **A judicial office holder should not save personal or sensitive information to any unencrypted device or use unencrypted memory sticks.**

3.3 Working out of the office

- 3.3.1 A judicial office holder may need to work on electronic files outwith SCTS buildings. If a judicial office holder has a stable internet connection (e.g. at home), SCTS recommend the use of the VPN. This allows the judicial office holder to access all SCTS services from the laptop as if from the office. Email (via MS Outlook), internet browsing and working with files (MS Word) from the P:/ drive is the same as in the office once the VPN connection is established.
- 3.3.2 A judicial office holder may need to work somewhere with no stable internet connection (e.g. train). If so, he or she should transfer a subset of any active files to the local C:/ drive. See section above on [Saving Files](#).
- 3.3.3 Laptops should be shut down whenever they are transported outside SCTS buildings and other official premises. Passwords must not be stored with laptops or mobile phones.
- 3.3.4 Official devices such as laptops or mobile phones should not be left unattended. If judicial office holders need to do so, they must assess the risk. Phones and laptops should not generally be left unattended at a conference

⁴ dst@scotcourts.gov.uk

venue or on public transport. Thought should be given to ensure that devices are only taken outwith SCTS buildings when necessary.

- 3.3.5 When using laptops and mobile phones outwith SCTS buildings, extra care should be taken to avoid being overlooked or overheard.
- 3.3.6 Judicial office holders issued with official equipment are advised against working on official business using their own personal equipment.

3.4 Using Email services

- 3.4.1 Judicial office holders who have an SCTS-managed email account (Judges, Sheriffs) can access their mailbox via either their laptop or an SCTS issued mobile phone.
- 3.4.2 All email received in SCTS-managed email accounts is filtered to remove those emails which are likely to contain viruses or similar threats or are likely to be unwanted e.g. spam, phishing, ransomware. The filtering is based on frequently updated algorithms, though, on occasion unwanted email still gets through.
- 3.4.3 All email users must always assess the genuineness of all email received. For example a judicial office holder might ask himself or herself: was I expecting this email, does it feel right, is it enticing me to do something. Generally, unwanted email should just be deleted. However, if email is received that may be a credible and well-crafted attempt to elicit a response with the aim of extortion or fraud it should be reported to the IT unit at 0131 444 3333. Recent examples of email received by judicial office holders have included fake reports of a judicial complaint and fake attempts at sextortion. These emails may attempt to install ransomware or demand payments.
- 3.4.4 SCTS-managed email accounts have multiple email addresses attached. The address which a judicial office holder gives out to others will govern how any email is routed to him or her. Generally an email should be given as either jbloggs@scotcourts.gov.uk or jbloggs@scotcourttribunals.gov.uk (technically these are interchangeable).
- 3.4.5 If asked for an email address on a secure government network (formerly gsi or pnn) an email address can be given as jbloggs@scotcourts.pnn.gov.uk or jbloggs@scotcourttribunals.pnn.gov.uk.
- 3.4.6 Judicial office holders who use CJSM (Justices of the Peace and Tribunals Members) must be aware of the CJSM terms and conditions. When working with attachments sent by email the guidance in [Using Non SCTS Equipment](#) should be consulted.
- 3.4.7 Judicial office holders are advised not to use other email services such as Hotmail, Yahoo! mail, Gmail, AOL or similar, web-based email accounts, to send or receive sensitive data. This is because such email systems may provide weaker email filtering. They allow very little in the way of control or troubleshooting following a potential breach. For example, it would not be

possible to examine specific authentication and server logs from a public email service. It would be difficult to ascertain exactly who had access to what data when pursuing a potential breach.

- 3.4.8 Judicial office holders should be aware that storing judicial contacts in non-SCTS address books or contact lists, such as in Hotmail, is also a security risk and should be avoided. The same advice applies to all similar email accounts. If an account is compromised it would reveal the address book to an attacker, who may then attack those listed or attempt to exploit the relationship (this is how the “I am stuck in a foreign hospital please send me money” scam, purporting to be from someone you know, operates and has been attempted on Scottish judiciary).
- 3.4.9 Judicial office holders are encouraged to bear in mind the legislation when writing about individuals in email correspondence. Should that individual make a Subject Access Request under the GDPR these emails may be released if they were written while the judicial office holder was not acting in a judicial capacity.
- 3.4.10 As a matter of courtesy, the Judicial Office will inform the judicial office holder concerned if a Subject Access Request has been made.

3.5 Using the Internet

- 3.5.1 Judicial office holders may access the internet from the SCTS network in support of their judicial duties, but should always bear in mind that, although it is a valuable source of information, there are a number of inherent risks associated with its use. Such risks include being tracked, receiving fake information, and being vulnerable to malware such as ransomware and viruses.
- 3.5.2 Private use of the Internet via equipment provided by the SCTS is allowed. However, the extent and nature of that private use must be both reasonable and at all times entirely in keeping with the judicial office holder’s office and duties. The Lord President has agreed that the SCTS may apply web filtering software to accounts held by judicial office holders. The list of blocked categories is provided on the judicial intranet at:

http://judicialintranet/library/information/it/site_access.dochoholderscertain limits

- 3.5.3 This website also provides information on how a judicial office holder can either have a website reclassified, if it has been wrongly classified within the blocked groups, or gain access by stating a clear business need.
- 3.5.4 As a general rule, judicial office holders should bear in mind that IT facilities which are provided at public expense should never be used in such a way as to compromise the security of the machine, embarrass the judiciary as a whole, or bring a judicial office holder into disrepute. Improper use might be a matter dealt with under the 2017 or 2018 disciplinary Rules.

- 3.5.5 In the event of accidental access to an inappropriate site (for example through following a link from an internet search engine), the judicial office holder should use his or her discretion in deciding whether this should be notified to the IT Helpdesk to take appropriate action, e.g. run virus scans etc.
- 3.5.6 Although judicial office holders' web browsing activities are not routinely monitored, the IT system does record every webpage accessed. It enables searches to be undertaken, which can show all web pages that have been accessed.

3.6 Malware and Virus protection

- 3.6.1 Anti-virus software is installed and managed on all SCTS-managed devices provided to judicial office holders. This includes the distribution of up-to-date virus detection files to all managed devices. These updates can be issued several times a day to keep up with threats released on the internet.
- 3.6.2 While SCTS devices have centrally managed anti-virus protections, judicial office holders should be aware of the threat of viruses and other malicious software and of the procedures to recover from an infection.
- Anti-virus software must be installed on the computer and updated on a regular basis. It should never be disabled (centrally controlled).
 - Only authorised software from approved sources should be used. This reduces the risk, but does not eliminate it (centrally controlled).
 - A scan must be actively carried out on all connected media e.g. USB drives and CDs. While this is centrally configured, equipment users should ensure that these scans are carried out (a pop-up should report progress) and report any issues. To minimise the risk that only USB drives and CDs from trusted sources should be used. If using a personal USB drive, it should be used in as few machines as possible.
- 3.6.3 In the event of a suspected or actual virus infection, the following actions should be taken:
- Do not attempt to continue using the machine.
 - If using SCTS equipment between 8:30 and 5:15 Monday to Friday a judicial office holder should phone the SCTS IT helpdesk immediately on 0131 444 3333. If working out of hours, he or she should contact the helpdesk at the earliest opportunity.
 - The judicial office holder will be asked to note what actions/functions were being carried out when the virus was discovered.
 - The judicial office holder will be asked to note any screen messages (e.g. error messages) or actions taken by the computer.

- The judicial office holder may be asked to disconnect from the network. If working out of hours, or if the IT helpdesk cannot be accessed immediately, disconnect from the network.
- Advise any colleagues to whom emails may have recently been sent an email who may have received emails from the same source.
- Draw up a list of all those to whom emails may have been sent, and from whom infected disks or email may have been received.

3.6.4 It is possible that, following any confirmed malware issue, a judicial office holder will be asked to change any passwords that may have been compromised. It is also likely that SCTS will seek to take away old equipment to be completely wiped. If that occurs new equipment will be provided.

4 TRAVELLING ABROAD

4.1.1 SCTS laptops and mobile phones should only be taken abroad if there is a business need to do so. They should not be routinely taken on holiday. Different countries pose different risks to information security from both official and unofficial sources. Countries have differing laws on the lawful use of cryptography. A judicial office holder may be asked to unencrypt devices by entering the password to allow the device to be examined. This will reveal all device contents and could constitute a data breach. If a judicial office holder wishes to process judicial data outside the UK he or she should contact the Judicial Office in advance to clarify if there are any potential difficulties. Further advice is available from the IT Unit.

4.1.2 For judicial office holders wishing to process judicial data outside the UK, the SCTS can offer a standalone device which allows connectivity and work on active files but which, if compromised, would not compromise the wider SCTS network. If asked to open the device, the access given should be as limited as possible.

5 USING NON SCTS EQUIPMENT

5.1.1 SCTS strongly suggest that judicial office holders process all data relating to their judicial office using equipment provided by SCTS.

5.1.2 Where the judicial office holder works on non-SCTS equipment or their personal equipment, the following minimum security controls are recommended:

- Equipment should only be bought from a reputable source. Second hand or free equipment, for example free USB drives given out at events, should be avoided. The device's operating system should be up-to-date, currently supported by the software company and have security patches applied regularly.
- The device should have anti-virus software installed, up-dated and running.

- The device should have full disk encryption (minimum standard for AES256).
- The device must require unique authentication; e.g. a username and password or fingerprint.
- The device should not be operated daily using administrator permissions. The built-in administrator account can be used to create a standard user account. If a virus is picked up it can usually only operate in the context of the user who got infected. Running as a standard user will often limit the impact whereas running as administrator will give the virus full control of the device.
- Limit the software installed on the device to that from a trusted source; e.g. a reputable vendor, update software when the vendor offers new versions and removed software which is no longer needed.
- The device should not be shared with others; including family. If it is shared, there should be provision for files to be isolated and protected from other users.
- Information stored on the device should be kept to a minimum of active files. Case data will be retained by SCTS. A separate archive should not be necessary.

5.1.3 When no longer needed, the device should be securely wiped and disposed of. Do not pass the device on without being sure all data has been removed. The standard delete process should not be considered sufficient. Use of these computing facilities should be limited to activities involving data included in a draft opinion or judgment, reviewing documents and sending or receiving emails. Where there is a need to access large volumes of personal or protectively marked data, only SCTS computing facilities should be used. Removable media provided by SCTS must be returned to SCTS after use.

6 USING PERSONAL MOBILE PHONES

- 6.1.1 Many judicial office holders will hold personal details on his or her mobile phone including those of other judicial office holders. Precautions should include: not leaving them in cars or places where they might be stolen and ensuring that the keypad lock is activated.
- 6.1.2 In compliance with the legislation, any personal data must be deleted when no longer required. The appropriate period of retention should be considered. All sensitive and/or personal information must be securely disposed, of when no longer required.
- 6.1.3 Deleting a file will normally only have the effect of transferring it to the Recycle Bin. The Bin should be emptied at the end of sessions on devices which are not owned by the judicial office holder. Even if it is deleted permanently, someone with appropriate software can usually recover it and, unless it was encrypted, access it.

6.1.4 Computer hard disk drives should be securely erased before disposal or recycling if they have held any personal or protectively marked data. Please discuss any arrangements with the SCTS IT helpdesk.

7 USE OF SOCIAL NETWORKING

7.1.1 Judicial office holders should bear in mind that the spread of information and the use of technology means it is increasingly easy to undertake 'jigsaw' research which allows individuals to piece together information from various independent sources. Information about a judicial office holder's personal life and home address should preferably not be available online. A simple way of checking is by typing the judicial office holder's name into an internet search engine such as Google. A judicial office holder may want to talk to his or her family about social networking systems, such as Facebook where personal details which carry some risk (such as holiday absences) can unwittingly be put into the public domain). Access to Social Networking sites from computers on the SCTS network is blocked by default by the web filtering software.

7.1.2 The judicial office holder should:

- Be wary of publishing more personal information than is necessary. In particular phone numbers, dates of birth and addresses are key pieces of information for security fraudsters. Other users probably don't need to know such details. If any contacts do need them, it is advisable to send them to individuals separately.
- Posting some information could put a judicial office holder's personal safety at risk. A judicial office holder's address, details of holiday plans and information about his or her family, could be used for criminal purposes. Photographs could enable home addresses or car numbers to be identified.
- Check the privacy settings. The judicial office holder can restrict access to his or her profile to ensure the information is kept to a restricted group.
- Check the terms and conditions of any sites the judicial office holder signs up to, to ensure he or she is aware of who owns data posted on the site and what the owners of the site can do with this data.

8 CARE OF PAPER FILES

8.1.1 The judiciary work in a number of different ways. Some are based at a single court or tribunal centre. Others may have no official base and sit at more than one building in the course of a week. However at work the judicial office holder should adopt the most secure means of transporting documents available. The following should apply:

8.1.2 Where possible the judicial office holder should personally return documents to the court or tribunal and hand them to a member of SCTS staff. If there is

no bag service available, the judicial office holder should discuss alternatives with the sheriff clerk or equivalent.

- 8.1.3 Use a secure bag that can carry the weight of documents (lockable if possible). Documents should be kept in the judicial office holder's possession, unless that is impossible (e.g. because of their bulk). They should not be left in unsecured places such as tables in restaurants, cloakrooms or visible in a car.
- 8.1.4 Use fax machines as a last resort. Double-check the number to which documents are to be sent. If faxing to an open office, make sure that there is someone to collect and secure the fax at the other end (or ask them if there is a PIN code facility).

9 STORING PAPER FILES

- 9.1.1 Judicial office holders should take all reasonable steps to prevent access to personal data in their possession by people who are not authorised to see it. When working from SCTS premises, the most effective way to do that, if possible, is for documents to be locked away securely, especially overnight. Administrative staff must provide the judicial office holder with adequate secure storage facilities whether he or she is a permanent or visiting judicial office holder.
- 9.1.2 If it is not feasible to lock papers away at the end of the day or during the day (because of the quantity) the judicial office holder should speak with a member of SCTS staff to agree alternative arrangements.
- 9.1.3 The SCTS staff will make sure that adequate door locks (either key operated, or combination, or possibly both) are provided.
- 9.1.4 In some locations the presence of other security arrangements may obviate the need for documents to be locked away. If the chambers are in a secure area to which access is limited by a pass card, this will ensure that access to a judicial office holder's chambers will be only by people with a key, or by those who know the security code for a combination lock, or who have a pass card.
- 9.1.5 SCTS staff do not need to be forbidden from entering chambers in the absence of the judicial office holder solely to prevent access to information. It is highly likely that the SCTS is a joint data controller for any personal data which the judicial office holder may have. SCTS staff are authorised to have access to it. They may enter locked chambers in order to deliver or retrieve papers as agreed with the judicial office holder in the ordinary course of business. Contractors who are allowed to work unsupervised by SCTS may be given access. They are bound by the terms of the contract they have with the SCTS to ensure that protected data is not disclosed.
- 9.1.6 Judicial office holders have to consider fully, in the light of this guidance, the extent to which they can allow access to his or her chambers by parties or their lawyers or other visitors without ensuring that protected data cannot be seen or accessed.

10 DISPOSAL OF PAPER FILES

- 10.1 Court or tribunal papers must be handed to the clerk of court, macer or court officer for effective disposal. Alternatively, the confidential waste bins that are located around court premises should be used.

11 LINKS TO SCTS GUIDANCE

- 11.1 Although not applicable to the judiciary, the SCTS guidance on information risk management may be useful as a further reference point:

http://myscs/library/people/policies/Information_Risk_Management_2011.doc

- 11.2 This guidance will be reviewed on a regular basis. Any comments or suggestions as to the content should be sent to the Judicial Office.

Data Breach Notification Form

When to use this Form

This form **must** be used when you become **aware** of a suspected data protection breach or an actual data protection breach.

It must be filled in with as much detail as possible and sent to the Judicial Office as soon as you become aware of the suspected/ actual data breach.

You must act as soon as you become aware of the suspected/ actual breach. This is because the Information Commissioner must be notified of a relevant breach within 72 hours of you becoming aware of a breach that is likely to result in a risk to the rights and freedoms of individuals.

Completing the Form

The Form is in two parts:

- Part 1 must be completed by the person reporting the breach
- Part 2 must be completed by the Judicial Office

Part 1 – to be completed by the person reporting the breach

Name of person reporting the breach		
Date and time of breach, if known		
Who discovered the breach?		
Date and time the person who first became aware of the breach became aware		
Date and time person first became aware of the breach reported it to:	Judicial Office and SCTS data breach centre:	
	Sheriff Principal/ Chamber President/ President of Scottish Tribunals/ Lord President: (delete as appropriate)	
How was the breach discovered?		
Describe the breach, how it occurred, and data involved, any third parties involved <i>Give as much detail as possible</i>		
Describe the categories of data involved in the breach		
Does the breach concern special category data? If so, which categories?	<ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Data concerning health • Data concerning a natural person's sex life • Data concerning a natural person's sexual orientation <p><i>Delete those not applicable</i></p>	

Describe the approximate number of data subjects affected by the breach	
Describe the approximate number of personal data records affected by the breach	
Deadline to report to Information Commissioner/ DP Supervisory Judge (72 hours from the time person who first became aware of the breach became aware of it)	

Once Part 1 is completed the Form must be sent to the Judicial Office at judicialofficeforscotland@scotcourts.gov.uk and SCTS data breach team at databreach@scotcourts.gov.uk

Part 2 – to be completed by the Judicial Office

Judicial breach number of 20.....
Name of official in Judicial Office	
Date and time received by Judicial Office	
What are the likely consequences of the personal data breach?	
What measures have been taken or will be taken by the data controller to address the breach, including measures taken to mitigate adverse effects of it?	
Is the breach <i>likely</i> to pose a high risk to the rights and freedoms of individuals? (Y/N)	
In the event of a breach or suspected breach that is likely to pose a high risk to the rights and freedoms of individuals, the following have been informed	<ul style="list-style-type: none"> • LPPO • JO Comms Team <p><i>Delete as inapplicable</i></p>
Does the breach arise in respect of data processing that has been carried out by a court, judge or tribunal acting in its judicial capacity? (Y/N)	
Date and time reported to the ICO or the DP Supervisory Judge	
If not possible to report within 72 hour deadline explain why	
Details of breach entered on Judicial Data Breach log? (Y/N)	
Actions taken by Judicial Office, with date and time, to contain the breach, recover data, investigate any operational or structural changes or training required to minimise future breaches	
Insert date of completion of Table 2	