LORD CHIEF JUSTICE OF ENGLAND AND WALES

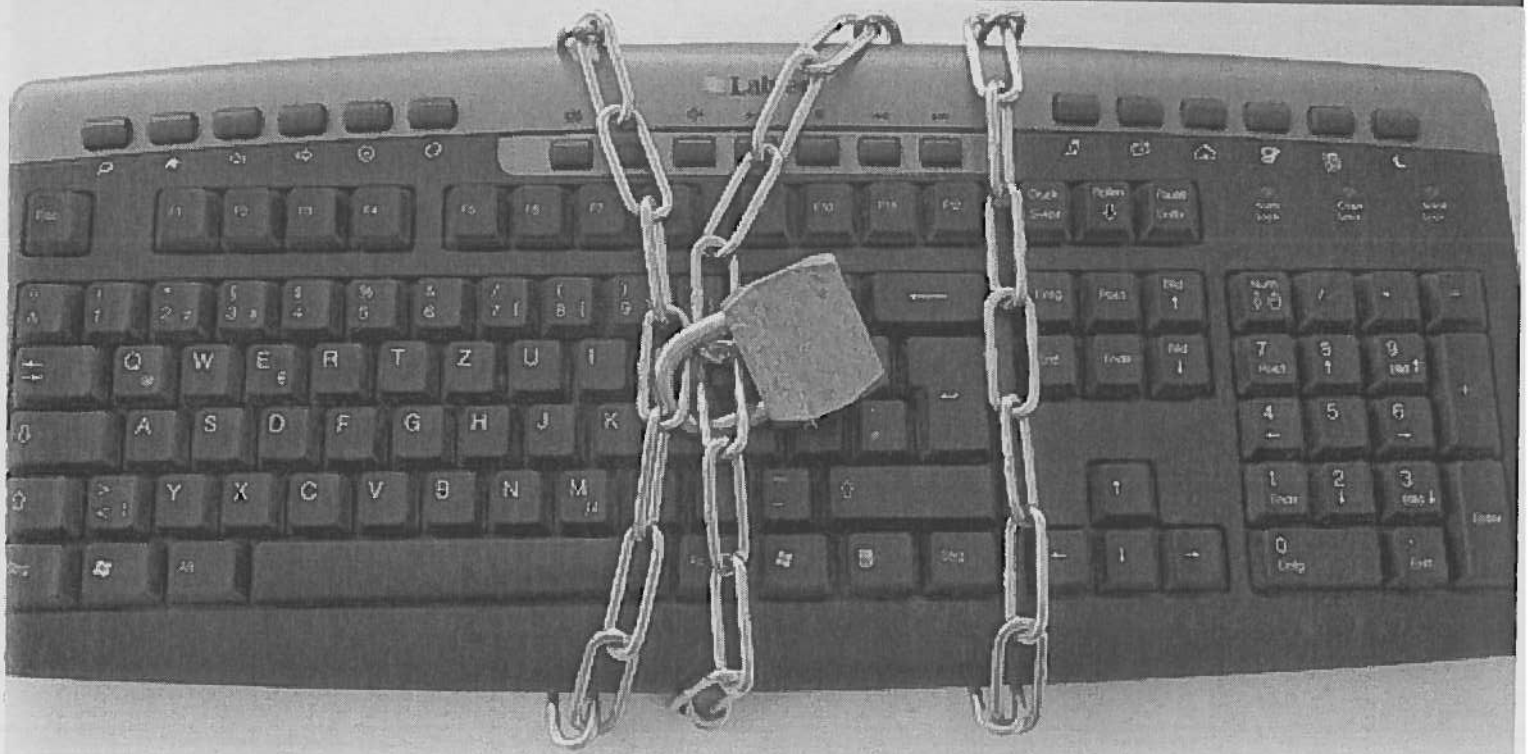
SENIOR PRESIDENT OF TRIBUNALS

The Responsibilities of the Judiciary

Part 1: A Guide to the Data Protection Act 1998

Part 2: Data Loss and IT security

Part 3: Managing Data Loss



September 2015

Contents

Introduction

This guidance comes in three parts, which were previously dealt with in a separate document. It applies to judicial office holders in the courts in England and Wales, and those judges and members in tribunals which fall within the responsibility of the Senior President of Tribunals.

- The first part explains how the Data Protection Act 1998 (DPA) applies to judicial office holders.
- The second part includes guidance on IT and document security.
- The third part sets out what to do in the case of any data loss.

This guidance sets out practical and proportionate ground rules for the judiciary. None of it is particularly new or unexpected and much of it you will already do as a matter of course. However, it is important that all judicial office holders read this guidance. This is particularly so in light of the potential consequences of failing to follow the guidance, which could include disciplinary proceedings and personal liability for the decisions made. This could in, some circumstances, include responsibility for payment of a civil monetary penalty should one be imposed by the Information Commissioner.

This revised guidance is issued with the agreement of the Lord Chief Justice and the Senior President of Tribunals.

Part One
A guide to the Data Protection Act 1998

1. Judicial office holders as Data Controllers

1.1 Individual judicial office holders are data controllers in circumstances in which they, either alone or jointly or in common with other persons, determine the purpose for which, and the manner in which, any personal data is or will be processed. This applies to data processed in the exercise of any judicial functions, both adjudicative and non adjudicative, and including any appointment, disciplinary, and leadership functions.

1.2 Data has a specific meaning for the purposes of the DPA, as set out in **Annex A**. There are two categories of data that fall within the scope of the DPA: personal data, and sensitive personal data.

1.3 There can be more than one data controller in a particular instance. For example, where you are one of three judicial office holders in a constitution, you are each likely to be a data controller in your own right. There will also be a number of instances where both the judiciary and another individual/ organisation are data controllers or act as data controllers at different stages of a given process.

1.4 This means that you are required to ensure the safe custody of:

- personal data you obtain through exercising your judicial functions;
- personal data you have acquired through your judicial role; and
- personal data you are processing for which the MoJ, HMCTS or another party (e.g. the CPS) might jointly be the data controller.

This applies to hard copies of documents as much as to electronically stored information.

1.5 There is no need for a judicial office holder, when exercising judicial functions, to register as a data controller with the Information Commissioner[1]. However, judicial office holders remain subject to the requirements of the DPA which fall on data controllers generally, as set out in paragraph 3 below.

1 Under the DPA data controllers are required to notify the Information Commissioner when processing data and pay a notification fee. They are then added to the register of data controllers. Judicial office-holders are exempt from this requirement where they are processing data for the purpose of exercising judicial functions by virtue of the Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 SI 2009/1677.

2. Handling Subject Access Requests

Receiving a request

2.1 Under section 7 of the DPA, individuals can request access to their personal data, subject to exemptions (see **Annex C**). A request must be made in writing and is known as a Subject Access Request (SAR).

2.2 Judicial office holders, where they are the data controller of personal data, are expected to approve responses to Subject Access Requests (SARs).

2.3 If you receive a request personally you should immediately refer it to the Knowledge and Information Liaison Officer (KILO) for your local area (KILOs are based regionally and a list can be found at the end of **Annex C**). A KILO is a nominated member of staff who has responsibility for co-ordinating responses to requests made under the Freedom of Information Act 2000 and the DPA.

2.4 If this person is not known to you, you should refer the request to the senior member of staff at your court or tribunal. They must refer the request to the Ministry of Justice's Data Access and Compliance Unit (DACU) who will provide further advice if needed.

2.5 Alternatively, you can refer a request direct to DACU at Data Access & Compliance Unit, 10th Floor, 102 Petty France, Ministry of Justice, London SW1H 9AJ or
or by fax to

Preparing a response

2.6 It is necessary to identify what, if any, personal data is held in relation to a data subject. The requirement is to provide a data subject with a copy of all of the personal data held (subject to any exemptions) in an intelligible form, but not every document in which that information appears.

2.7 If the data subject is a party to a case then, depending on the type of case before the court or tribunal, if appropriate, it may be sufficient to satisfy the requirements under the DPA if the requesting data subject is sent a copy of the open case papers. This is because judges (and HMCTS officials) will usually hold personal data about the data subject as a result of it being provided in such documents

2.8 It follows that it will not normally be necessary to provide the data subject with copies, or a description, of internal communications regarding a case. This is because such documents are unlikely to contain any additional personal data in relation to the data subject which is not duplicated in the open case papers.

2.9 Some internal documents may include a record of the judge's reasoning, including the application of legal principles to the facts of the case, and analysis of the arguments put forward by each party. There is authority to say that legal analysis, including application of the particular facts to the

legal framework, does not constitute personal data. The underlying facts on which the legal analysis is based may amount to personal data, but such data is likely to be available within the open case papers.

2.10 This is relevant to documents like draft judgments and emails between judges determining a case, as well as judges' notes of proceedings.

2.11 However, where internal communications contain personal data not duplicated within the open case papers, or personal data that does not amount to legal analysis, it may be necessary under the DPA to provide the data subject with a copy of the personal data in question.

2.12 Judges should be aware of the possibility that a subject access request may result in disclosure of private comments about individuals.

2.13 Handwritten notes placed on the court and tribunal file are unlikely to form part of a relavant filing system for the purposes of the DPA and do not need to be disclosed under the DPA[2].

2.14 Judicial office holders should be consulted before internal communications involving them are disclosed, even where they are not the data controller. The officials preparing the response in these circumstances should have regard to the judicial office holder's views about a response.

2.15 **Annex C** provides more detail about preparing responses to SARs and should be read in conjunction with this section.

3. General responsibilities imposed by the Data Protection Act 1998

3.1 The DPA uses terms such as 'data', 'personal data', 'sensitive personal data', 'processing', 'data subject', 'data processor' and 'data controller'. These terms are explained in **Annex A.**

3.2 The DPA states that anyone who processes personal data must comply with the eight Data Protection Principles. These are set out in Schedule 1 to the DPA and require that personal data is:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and, where necessary, kept up to date;
- Not kept for longer than is necessary;
- Processed in line with the data subject's rights;

2 This point is currently be considered by the Information Commissioner and may need to be reconsidered in due course.

- Secure; and
- Not transferred to other countries without adequate protection.

3.3 The principles apply to all personal data unless subject to an exemption under the DPA.

3.4 **Annex B** explains the data protection principles in more detail.

Exemptions

3.5 The DPA provides exemptions (i) in respect of data that would otherwise fall to be disclosed under a SAR and (ii) for permitting disclosure of personal data that would otherwise be in breach of the DPA. These fall into two categories:

(i) the "subject information provisions"; and

(ii) the "non-disclosure provisions".

3.6 **Annex C** sets out more detail about the exemptions from the subject information provisions.

3.7 Exemption from the non-disclosure provisions is available in circumstances where the DPA recognises that the public interest requires disclosure of personal data that may otherwise breach the DPA.

3.8 Disclosures which are required by law or are necessary in connection with legal proceedings are exempt from the non-disclosure provisions.

3.9 There are further exemptions from the non-disclosure provisions that would be too lengthy to set out for the purposes of this guidance.

3.10 If you are in any doubt, the KILO or DACU may be able to seek legal advice from a MoJ lawyer, or from the KILOs in the Judicial Office who deal with such requests on a more regular basis.

4. Enforcement and Failure to Comply with the Data Protection Act

4.1 The regulatory powers of the Information Commissioner are set out at **Annex D**.

4.2 The Information Commissioner has powers to investigate complaints about the processing of personal data under the DPA. Complaints and breaches of the DPA may also be considered under the existing procedures for dealing with complaints about judicial misconduct, under the auspices of the Judicial Conduct Investigations Office, or may lead to court or tribunal proceedings.

5. The Freedom of Information Act 2000 [FOIA]

5.1 Some requests for information will say that they are made under both the DPA and the FOIA. It is important that when this happens, responses cover both types of request.

5.2 However requests for information may be valid even if they do not refer to specific legislation. It is important that the request is read carefully.

5.3 Information for the purposes of the FOIA is not restricted to personal data.

5.4 Again, a KILO or DACU will be able to give advice on the most appropriate way of responding to any such requests.

Part Two
IT and Document Security

1. Application

This section of the document provides guidance for all judicial office holders on the use, transport, storage and disposal of personal or sensitive information.

These ground rules apply to handling both personal data and sensitive personal data, and where other material you are handling is sensitive. It covers material in all tiers of the Government Security Classification Policy.

This guidance therefore applies to any material that falls within those parameters – whether it is judicial, personal files, or court files and whether they are in hard or soft copy. You will note that the DPA has more restricted definitions of "personal data" or "sensitive personal data" (see Annex A). This guidance encompasses, but is not restricted to, data falling within both definitions.

2. Responsibilities

2.1 You must take responsibility for understanding the risks associated with how you handle personal data or other sensitive data. No method of storage, transmission or transport of information can be 100% infallible – accidents and incidents will always occur - but risks must be minimised. Actions should be proportionate to the sensitivity of the information being handled.

2.2 You are required to ensure the safe custody of all information and personal data for which you are data controller or that is in your possession. You must also ensure you keep safe all information including personal data that is processed by you, and belongs to you or other people or departments (for example the Ministry of Justice, Crown Prosecution Service, Home Office, appellant or respondent in a case).

2.3 In the unlikely event that you cannot work within this guidance you should contact the senior judge in your area (i.e. Senior District Judge (Chief Magistrate), Bench Chair, Chamber President, Regional Tribunal Judge or Resident Judge) to make alternative and case specific arrangements.

3. Staff

3.1 Please bear in mind that Civil Servants are subject to strict Cabinet Office and MoJ guidance on information security. They may be subject to disciplinary action if they breach that guidance so do not press them to do something which puts them in an impossible position.

4. Security Classifications

4.1 The Government now uses a three tier system for classifying information handled in the context of government business (OFFICIAL, SECRET, and TOP SECRET). See **Annex E.**

4.2 For more detailed information on the classifications see:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

4.3 In most contexts, and unless it is specified by the business owner of the information, indicated by the business context or parties to a particular case, or directed by the judicial office holder(s) themselves, information handled in normal business will be treated as OFFICIAL.

4.4 Judicial office holders who receive SECRET or TOP SECRET documents will be provided with instructions as to how they are to be safeguarded. Such documents must never be sent by email or stored on standard departmental desktops or on your own device.

4.5 Further advice on security classifications and handling requirements may be sought from local HMCTS staff or from the HMCTS Information Assurance Team (contact details can be provided by HMCTS staff).

5. Care of paper documents

5.1 Judicial office holders work in a number of different ways – some are based at a single centre whereas others may have no official base and sit at more than one venue in the course of a week. However you work, you should adopt the most secure means of transporting documents available to you. If it is necessary to take documents home or work on them in transit, the following should apply:

- Take only the minimum amount needed to enable work to be done;
- Keep documents secure when travelling and at home;
- When travelling, papers and files should never be left on show or unattended;
- Avoid taking indirect routes and avoid interruptions to journeys if possible

- Where possible, documents may be sent by post or approved courier services to/from your home, or to any HMCTS building where you will be working. A member of staff should be able to help with the arrangements and ensure that the method used conforms to HMCTS standards;
- Documents should be carried in a secure bag suitable for the weight (lockable if possible);
- Documents should be kept with you unless that is impossible (e.g. because of their bulk) and should not be left in unsecured places such as on tables, in restaurant cloakrooms or visible in your car;
- Unless there is no other option (i.e. because you are staying in a hotel and the papers are too bulky to keep with you) documents should not be left in a car overnight, even if they are locked out of sight;
- Fax machines should only be used as a last resort; double-check the number you are sending documents to. If faxing to an open office, make sure that there is someone to collect and secure your fax standing by at the other end (or ask them if there is a PIN code facility).

6. Storing paper documents

6.1 When working from HMCTS premises sensitive materials must always be locked away and other paperwork should always be stored or stacked away in a manner which minimises the accidental disclosure of private information. Administrative staff must provide you with adequate secure storage facilities whether you are based there permanently or visiting.

6.2 If it is not feasible to lock papers away at the end of the day, or during the day, a member of staff will arrange for your room to be locked or agree alternative arrangements with you.

7. Disposal of paper documents

7.1 Court papers must be either be handed to your court clerk, usher or hearing centre staff for disposal or placed in the confidential waste bins that you will find around HMCTS premises.

(**Note:** arrangements that apply for the disposal / deletion of electronic records are equally important and are provided in the relevant eJudiciary guidance)

8. Information Technology guidance

8A. Using your own device (i.e. Computers, Tablets, Mobile Phones)

8A.1 The introduction of eJudiciary makes it possible for judicial office holders to use their own devices or other private or business PCs / laptop, or open devices provided by MoJ, or, on an interim basis, DOM1 devices (either web based or by installed software) to access the eJudiciary system, subject to complying with this guidance and the following key principles.

- Ensure that the hard drive/storage is encrypted
- Only use your own device; don't trust other devices

- 'Approach & use' / openly shared devices (e.g. in hotels and internet cafes) should never be used for judicial business / e-Judiciary material. If you have to work on a computer and in an account to which others have access, it would generally be wise to work on the web (webmail and web-based versions of MS Office) because less information, or less readily accessible information, will be stored on the computer when you log off
- Set a password on the device
- Set a timeout lock on the device requiring a password to re-access the device
- Ensure that all software used is up to date so that security patches are timeously applied
- Install and enable and keep up to date anti-virus and anti-spyware where applicable
- Enable a device firewall where applicable
- Where possible, make sure that only you have administrator privileges for the computer you are using

- Where possible (e.g. on a PC) you should use a non-administrator account, to which only you have access, for using e-Judiciary and dealing with judicial matters, particularly if storing anything on the computer.
- Delete the browser history when using somebody else's computer or other such device.

- In respect of tablets and mobile phones (which are vulnerable to being lost or stolen), it is important to: 1) log into the device using the appropriate account for that device, 2) set up tracking, and, 3) familiarise yourself with the web-based track, ring, lock and erase facility

Please refer to your own device operating requirements document for further information.

If you are working on a file on an encrypted memory stick, you should not transfer the file to your computer hard disc, but instead work on the file as stored on the memory stick using encryption software.

Remember that deleting a file on your personal computer /device will normally only have the effect of moving it to the 'Recycle Bin' on the computer/device. Recycle bins should also be deleted. Even if you delete it permanently, someone with appropriate software might be able to recover it, and, unless it was encrypted, can access it.

Computer hard disk drives should be securely erased before disposal or recycling if they have held any personal or sensitive data.

Repairs or maintenance to personally owned devices must be undertaken by an established, reputable, and trusted firm or technician. A record /receipt referring to the work undertaken should be retained in case a security incident arises in the future which requires clarification of any access made to data on the device.

8B. Transporting electronically stored OFFICIAL / OFFICIAL-SENSITIVE information

8B.1 You may want to work with electronically stored information on your own device, for example to work on a draft judgment or summing-up.

8B.2 There are the following ways of transporting files from one computer to another:

(i) **eJudiciary:** The safest means of making information available away from your workplace is to save the file to your eJudiciary account and then access it on eJudiciary once at the other location, e.g. home. It can then be accessed again from your MoJ computer when you next need to.

If eJudiciary is accessed on a phone or tablet then potentially a thief (or finder) would have access to all the owner's emails (and any stored documents) in the same way they would on a computer. It is therefore particularly important that such devices are protected by pass codes and, where possible, encryption.

(ii) **Email the file as an attachment:** Emails containing sensitive information or personal data should only be sent over the Internet if the information is protected. The content of documents and emails sent over the Internet is as accessible to others as, say, messages written on postcards. Many people could read them (including internet service providers, telecommunications staff and malicious users) unless they are secured by encryption. The extent to which this is a risk to personal data is something

that judicial office holders are expected to determine themselves.

Some email routes encrypt the document en route and so are safer.

- email from one eJudiciary account to another is encrypted, as are emails from eJudiciary to a gsi account.
- email from a gsi account to an eJudiciary account is not encrypted;
- email from eJudiciary to a CJSM account is not encrypted.

Some third party accounts provide for encryption en route, both ways. This is true of hotmail.co.uk and yahoo.com, but not (for example) iCloud.com and zoho.com. Judicial office holders should ensure they know what the position is for any third party account they send information to, or use to receive information.

It is all too easy to send an email to the wrong recipient, particularly if you use the automatic complete facility when typing in the email address so care is needed. There is an implicit responsibility to ensure that you have the correct contact details.

(iii) **Copy the file to an encrypted memory stick:** The ability to store and access files centrally under e-judiciary means that it should seldom be necessary for a memory stick to be used. However for the circumstances where sensitive information cannot be saved and retrieved, or transferred via eJudiciary, or emailed securely, encrypted memory sticks are available.

- **Note:** Alternative solutions exist, but users must be clear on how secure any alternative is. For example, it is possible to create an encrypted stick using Bitlocker, but individuals are accountable for implementing such solutions correctly and effectively.

Anyone wishing to order an encrypted memory stick should apply to **support@ejudiciary.net** who will deal with applications.

Unencrypted memory sticks pose a significant risk if lost and should not be used if the information/ document is of any sensitivity. The information should be protected by using one of the alternative methods detailed above.

8C. Avoiding Viruses and Malicious Software

8C.1 All judicial office holders should be aware of the threat of viruses and other malicious software ('malware') and of the procedures to recover from an infection, and the key points below:

- Anti-virus software must be installed on the computer and must be kept up to date.
- Anti-virus software should never be disabled.
- Only software from established and reputable sources should be used. This reduces the risk of malware, but does not eliminate it.
- Anti-virus software should be set to automatically check all incoming data.

8D. Using the Internet

8D.1 When accessing the Internet, whether using MoJ provided equipment or a user-owned device, judicial office holders should ensure that the facilities are never used in such a way that they may compromise the security of the computer/device, embarrass the judiciary as a whole, or bring the judicial office holder personally into disrepute.

8D.2 Judicial office holders accessing Internet facilities 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 vulnerability to hacking of information held on connected machines and infection by viruses.

- Judicial office holders must use their judgement in determining whether or not a web site, chat room or newsgroup is inappropriate. **Accessing of inappropriate sites could be a disciplinary matter referable to the Judicial Complaints Investigation Office and, in certain circumstances, the police.**
- If judicial duties require access to an inappropriate site a judicial office holder should seek advice from the appropriate judicial authority. In the first instance, please discuss this with the senior judge in your area. You can also contact the SPJ's/SPT's office if you are in any doubt.
- 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 appropriate judicial authority.
- Users should be aware that browsing activity and searches can be subsequently tracked.

8E. Email content

8E.1 Although there is no specific guidance on this matter, judicial office holders are encouraged to keep in mind the Principles of the DPA when writing about individuals in email correspondence; should that individual make a Subject Access Request under the DPA these emails may be released.

8F. Use of social networking

8F.1 Judicial office holders are encouraged to bear in mind that social networking creates a public profile and is probably best avoided whilst in office. If you do use social networks bear in mind that the spread of information and use of technology means it is increasingly easy to undertake 'jigsaw' research which allows the piecing together information from various sources. **Under no circumstances should sensitive data be placed on any social network.**

- Try to ensure that information about your personal life and your home address is not available online. A simple way of checking can be by typing your name into an internet search engine such as Google. You may also want to talk to your family about social networking systems, such as Facebook, where personal details which carry some risk (for example, holiday absences) can unwittingly be put into the public domain.

- 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 send them to individuals separately.

- Posting some information could put your personal safety at risk. For example, your address, details of holiday plans and information about your family could be used for criminal purposes. Photographs could enable home addresses or car numbers to be identified.

8F.2 You should also:

- Check your privacy settings. You can restrict access to your profile to ensure your information is kept to a restricted group.

- Check the terms and conditions of any sites you sign up to ensure you are aware of who owns data posted on the site and what the owners of the site can do with your data.

- We are aware that some judicial office holders hold non-commercial directorships. In such cases, Companies House will need the individual's home address. This information is shared with third parties. You can, however, request that such information is not divulged.

9 Judiciary with MOJ equipment

9A Daily use

9A.1 Leaving your computer on and unlocked when you leave your room means that anyone who comes in may have access to your information on your hard drive or any networked drive. Unless you have confidence in the security of all those who might have access, you should at least apply the electronic lock when you leave it unattended. This is done by pressing Windows and L or Control Alt and Delete simultaneously and selecting "Lock computer". The computer is unlocked by inputting your DOM1 password.

9A.2 Whenever a laptop is unattended (e.g. when someone else could gain access to it, as in the situation above) it should be physically secured.

9A.3 It is imperative that you shut down your computer overnight, or when it is being transported but is not in use. Logging off is insufficient because it leaves the hard disc unlocked, unprotected and insecure.

- The hard discs of all MoJ provided computers now have encryption. However, the disc is only secure when the computer is shut down. If it is left on during your absence, or if it is transported in stand-by or sleep mode the data on the disc is not protected, and its contents may be accessed by unauthorised persons without too much difficulty. Depending on your version of Windows, hibernation mode may or may not protect the data on the hard disc and so it is best to assume it doesn't.

9A.4 The USB dongle should be removed once you have logged in, and the meaningless password, if written down, must be kept securely away from the computer.

9A.5 MoJ mobile computers have a personal drive (H drive), which is synced to hard drive of the computer to allow offline work. When the computer is attached to the DOM1 network (via broadband or network cable) the local copy of the personal drive can be synchronised with the network (it is automatically synced when disconnected/reconnected from the network). All network information is automatically backed up overnight. It is important to bear in mind, however, that if a document is stored on a memory stick, there will be no backup or copy unless you have made one; loss of or serious damage to the memory stick will mean loss of the information on it. If information is stored on the hard drive but not otherwise backed up, and the laptop is lost, the data will of course be lost too.

9A.6 In the event of a laptop failure or disk failure, recovery of data is at best very expensive and often impossible. It is important therefore to ensure that files are saved to network drives or that the laptop is regularly connected to the network to allow files to be backed up overnight.

9B. Using MoJ Laptops out of the office

9B.1 Laptops should be shut down to encrypt the hard drive whenever they are transported outside official premises. Do not keep your Becrypt/X-kryptor tokens or your password with your computer. Placing your laptop in the boot of a car is not safe storage for these purposes.

9C. Travelling abroad

9C.1 MOJ laptops should only be taken abroad if there is a business need to do so. Telephone systems are not considered to be secure and data security cannot be guaranteed using a dial up connection. The network should only be accessed via an approved secure connection using X-Kryptor (typically used to allow connection to the network via broadband).

9C.2 Different countries have different risks to information security. Some countries are assessed as sufficiently trustworthy; others are known to have active criminal or state sponsored electronic surveillance programmes of high capability. Since national threat profiles change over time, rather than give advice relating to specific countries in a guide whose contents change infrequently, the advice is to seek guidance via MoJ's Operational Security Team in the first instance.

Part Three
Managing Data Loss

1. What is data loss?

1.1 A loss of data could take many forms and you could discover it in different ways. The list below is not exhaustive but examples include:

- loss of a court/tribunal file, or one turning up where it should not be;
- theft or loss of a computer containing personal data;
- leaving a document or computer disk or memory stick containing personal information on a train or in any non-secure environment;
- the inadvertent release of personal details in an email chain; or
- allowing a third party (e.g. a family member) access to your device in such a manner as allows them access to personal data.

1.2 We all have a duty to safeguard confidential and personal information from unauthorised disclosure. The steps that should be taken to fulfil that duty will vary with the importance and sensitivity of that information. The information held by the judiciary on their computers (personal and MoJ provided devices) and in hard form varies in its importance and in its confidentiality.

1.3 At one end of the spectrum is information that is already in the public domain, such as judgments/decisions that have been handed down and statutes and authorities that have been published. At the other end 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 Public Interest Immunity (PII) material about an anonymous witness who fears that disclosure of his identity will put him at risk of retribution, are examples.

1.4 In between these extremes is information that would infringe a person's right to privacy or which 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 that would be embarrassing if disclosed, such as a less-than-glowing reference on an applicant for silk or a judicial office.

1.5 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 we would be unhappy to lose, and would cause embarrassment and reputational damage, and possibly a duplication of work, but

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 between panel members for agreement or to officials for typing.

2. Senior Judicial Responsibilities

2.1 The Senior Presiding Judge [SPJ] has day to day responsibility for managing court related incidents of data loss. Chamber Presidents [CP] have day to day responsibility for managing tribunal related incidents of data loss in respect of the Chamber which they preside over.

3. Responsibilities of judicial office holders: What to do if you lose data

3.1 It is important that, when a loss of data first comes to light, you immediately report the incident to the office of the SPJ or relevant CP so that they can co-ordinate the response.

3.2 You should also inform your senior judge locally (i.e. Senior District Judge (Chief Magistrate), Bench Chair, Chamber President, Regional Tribunal Judge or Resident Judge) and inform local HMCTS management if the data lost is HMCTS information or of relevance to HCMTS business or proceedings for which HMCTS is, or may be, a joint data controller.

3.3 This guidance sets out the process for doing so. It is designed to provide rapid assistance to any judicial office holder involved in a data loss incident in order to minimise the impact at the earliest opportunity.

3.4 The process for reporting data losses amongst the courts and tribunals judiciary is set out at **Annex F.**

3.5 The important thing is to respond speedily to any incident. The sooner it is reported the sooner action can be taken to recover the material or mitigate the loss.

4. Context

4.1 Observance of this guidance is important because the Information Commissioner has stated that the loss of any laptop or removable media which is not encrypted is likely to be found as a data breach. A serious breach could attract a large fine and/or criminal sanctions levied on the data controller responsible. There will be circumstances in which you as an individual are the data controller responsible for a given piece of information.

You could personally be responsible for any breach of the data protection principles. The MoJ will indemnify any judicial office holder (acting as a data controller) who is performing a judicial function and has followed this guidance. If you do not follow the guidance you risk personal liability (without indemnity).

In some circumstances an incident may be so serious it will be referred to the relevant Head of Division/SPT. A serious breach could be the subject of an investigation by the Judicial Complaints Investigation Office or Chamber President. The extent to which this guidance has been observed is likely to be a relevant consideration. Judicial Office Holders who have not followed the guidance may therefore be subject to disciplinary action.

5. What is the impact of the loss?

5.1 How "significant" a compromise is will depend on a number of factors and on the individual circumstances of a case. Examples of factors you will need to consider include: the impact on the individual; the number of people affected by the loss; whether or not there is media interest; and if anybody's personal safety is at risk.

A. High impact incidents

5.2 Incidents which involve risk to personal safety, exposure to fraud and/or identity theft, vulnerable individuals and loss of the personal data of more than 25 individuals are almost always high impact incidents.

5.3 Incidents which mean we cannot carry out our business, have an impact on a trial or a tribunal, involve damage to the reputation of the Judiciary, or could attract media attention will always be high impact incidents.

5.4 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.

B. Low impact incidents

5.5 Some incidents, for example a misplaced file within the office or a judgement/decision sent to the wrong individual and returned to the office the next day, can be managed effectively under the direction of, for example, the SPJ's office, Presiding Judge or Chamber President. Incidents involving a significant amount of personal data, for example involving more than 25 individuals, must **not** be classed as a low impact incident.

5.6 Low impact incidents that, on investigation, indicate a higher impact than first assessed must quickly be escalated via the office of the SPJ or the Chamber President.

5.7 Low impact incidents will be reviewed by the Judicial Office quarterly so that any trends or

Annex A
Definition of Data

---

1. Data

1.1 Definition

Data is defined in Section 1 (1) of the DPA. The key ways in which information can constitute data for the purposes of the DPA are where it is:

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

b) is recorded with the intention that it should be processed by means of such equipment,

c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

control weaknesses can be identified.

6. Email contact

6.1 It is important that there is a process for checking that all emails intending to draw attention to a data loss have been delivered and read. This can easily be achieved by using the delivery and read receipt facility on Outlook. To allow emails to be given priority they should include **'data incident'** in the title/subject **heading**. If in doubt, please telephone to confirm receipt of the email.

7. Judicial Press Office involvement

7.1 Data loss is a sensitive issue and a local incident may be of national media interest. Media responses must be cleared with the Judicial Press Office and if appropriate, Senior Presiding Judge or the Chamber President.

1.2 Information processed automatically

Information that is processed automatically includes all data held on a computer or held with a view to them being recorded on a computer or other automated system.

Such data could be contained, for example, in a simple MS Word file or an email on a laptop PC. Information could also include that which is held on databases used by HMCTS or the Judicial Office such as CREST, CASEMAN or FAMILYMAN. The definition also refers to data held on court tapes, be they the older analogue tapes or digital files.

1.3 Information recorded in a relevant filing system

For information to be recorded on a 'relevant filing system' and therefore held for the purposes of the Act, it must be held in an organised filing system structured either by reference to individuals or by criteria relating to individuals which allows ready access to specific information about a particular individual. In considering whether there is ready access to the information the key consideration is whether there is a system in place that enables the finding of the information without searching through every item in the set of information.

- **Example 1:** a system is created which uses judges' names as the file title. The file title is HHJ John Smith and the file is sub-divided by tabs into: non-sitting days; sickness records, official business, training. This is likely to constitute a 'relevant filing system'.

- **Example 2:** a system is created to hold a single category of information about judges e.g. non sitting days. The information is divided between 26 files labelled from A to Z. Each contains details of the number of non sitting days of the judges whose surname begins with the relevant letter of the alphabet. Under each letter the judges' details are held in alphabetical order by name. This is likely to constitute a 'relevant filing system'.

Chronological filing

Information falling into various different categories filed purely in chronological order is unlikely to be held in a relevant filing system because it is structured by reference to date rather than 'by reference to individuals or by reference to criteria relating to individuals'. Where a set of information contains only a single category or information held in chronological order it will not usually comprise a relevant filing system unless it is first referenced to individuals or by criteria relating to individuals.

- **Example 3:** a post room keeps a record of all correspondence it receives. Each piece of correspondence is copied by the post room before distribution and placed on a 'day file'. The 'day file' is filed purely in date order and the name of the file will simply be the date of the correspondence. This is not a 'relevant filing system' as a particular copy letter can only be found by searching through all documents in the 'day file'.

Limited structures

When considering whether records comprise a 'relevant filing system' it is important to bear in mind the amount of information that is held. Where there is relatively little information, it is more likely that there will be ready access to specific information about a particular individual and that therefore it is a relevant filing system.

The key consideration is whether the records are sufficiently well-structured to facilitate ready access to specific information about a particular individual.

Test

Determining whether information is part of a 'relevant filing system' will often require careful analysis. By way of assistance, the Information Commissioner has proposed a 'temp test':

> 'if you employed a temporary administrative assistant, would they be able to extract specific information about an individual without any particular knowledge of your type of work or the relevant documents you hold?'

1.4 Data recorded by a public authority

The definition of data under section 1(1)(e) of the DPA was inserted by the Freedom of Information Act 2000 (FoIA). Its purpose is to ensure that requests for information made under FoIA are subject to the DPA and thus offer protection to individuals' data. It covers recorded information held by a public authority which does not fall within the above categories.

Judges are not listed as public authorities for the purposes of FoIA and so information they hold will not fall within this definition of data.

2. Personal Data

Section 1(1) of the DPA defines "personal data" as data which:

- Relate to a living individual who can be identified from those data or from those data together with other information which is in or is likely to come into the possession of the data controller;
- Includes expressions of opinion about the data subject and any indication of the intentions of the data controller or any other person in respect of the data subject.

There are situations in which data obviously relates to a person. However in situations where it is less clear, it is useful to consider whether the data is being processed, or could easily be processed, to learn, record or decide something about an identifiable individual; whether as an incidental consequence of

the processing something could be learned or recorded about an identifiable individual; or whether an incidental consequence of the processing is that it has an impact or affects an identifiable individual.

A name contained within a piece of information may not by itself be enough to mean that the person can be 'identified' from the data. In simple terms, 'John Smith' may tell you very little about who Mr. Smith actually is in comparison to 'His Honour Judge John Smith'. Conversely, it may be possible still to identify the person from the data available, even if the name and address has been redacted or removed.

Finally, it should be noted that a given piece of information may contain the personal data of more than one data subject. For example, a psychology report may contain the personal data of both the patient and the report's author.

3. Sensitive Personal Data

Sensitive personal data is defined in section 2 of the DPA. It means personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- his political opinions;
- his religious or other beliefs of a similar nature;
- his membership of a trade union;
- his physical or mental health or condition;
- his sexual life;
- the commission or alleged commission by him of an offence; or
- any proceedings for an offence committed or alleged to be committed by him or the disposal of or the sentence of any court for such proceedings.

Annex B
Explanation of the Data Protection Principles

1. Fair and lawful processing of Data

The First Data Protection Principle requires that data be processed fairly and lawfully and in particular shall not be processed unless at least one of the conditions in Schedule 2 to the DPA is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the DPA is also satisfied.

The vast majority of processing which is undertaken for the purposes of your judicial functions will be for the purpose of the administration of justice and will therefore fulfil the condition set out in Schedule 2 paragraph 5(a) and Schedule 3 paragraph 7(1)(a) of the DPA.

2. Specified and lawful Processing of data

The Second Data Protection Principle requires that data 'be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'.

3. Use for Limited Purposes

The Third Data Protection Principle introduces a requirement only to process data insofar as it is needed for the purposes for which it was obtained e.g. if requesting information about individual judicial office-holders' out of court activities in order to better profile a circuit's workload, it would not be necessary to request information about religious beliefs.

4. Accuracy of Data

The Fourth Data Protection Principle provides that personal data shall be accurate and kept up to date. Section 14 of the DPA allows a data subject to apply for a court order that a data controller must correct, block, remove or destroy personal data if they are inaccurate or contain expressions of opinion based on inaccurate information. The court may furthermore require the data controller to notify a third party to whom the data has been disclosed of the rectification, blocking or destruction.

The DPA provides that this principle will not be regarded as contravened if the data controller has taken reasonable steps to ensure the accuracy of the data and if the data subject has notified the data controller that the data subject's view is that the data are inaccurate and the data indicate that fact.

5. Retention and Disposal of Personal Data

The Fifth Data Protection Principle requires that personal data shall not be kept longer than is necessary for the purposes for which they are being processed. You should keep the processing of personal data under review and delete data as appropriate.

6. Rights of data subjects

The Sixth Data Protection Principle provides that personal data shall be processed in accordance with the rights of the data subject under the DPA. The DPA (Paragraph 8 of part II, schedule 1) describes how the Sixth Data Protection Principle may be contravened. Judicial office-holders should, in particular, bear in mind that they may contravene the Sixth Data Protection Principle by –

Failing to provide information in accordance with a subject access request [section 7 DPA] (see Subject Access Requests); or

- Causing damage or distress to the applicant, if the data subject gives written notification of damage or distress, or failing to respond to such a notice within 21 days [section 10 DPA]. The data controller must, within 21 days of receiving the notice, provide a written notice to the requester stating that he has complied or intends to comply with the notice, or stating why he regards the notice as to any extent unjustified.

- SARs have been dealt with above. In the unlikely event that you receive a notification under section 10 DPA, you should also refer it to your KILO or court or tribunal manager.

7. Security

The Seventh Data Protection Principle requires that due care is taken to protect personal data against unauthorised or unlawful processing and to prevent accidental loss, destruction or damage to personal data.

8. Location

The Eighth Data Protection Principle requires that personal data is not transferred to other countries outside the European Economic Area without an adequate level of protection being provided.

Annex C
Subject Access Requests and Administrative Arrangements

1. What is a Subject Access Request (SAR)?
2. How should an SAR be dealt with?
3. How will the KILO/DACU deal with the SAR?
4. Should a response to the SAR be provided?
5. Does the Ministry of Justice, HMCTS or a judicial office-holder hold any information relating to the subject of this request?
6. Does any of the relevant information qualify as 'data' within the meaning of the DPA?
7. Does any of that data fall within the definition of 'personal data' or 'sensitive personal data' as set out in the DPA?
8. Who is the 'data controller' of this personal or sensitive personal data?
9. Does the DPA contain any exemptions which may be used so as to prevent the disclosure of personal data or sensitive personal data to the requestor?
10. Are there any other considerations?
11. Flow chart showing the administrative process and timelines involved
12. Knowledge and Information Liaison Officer (KILO) list

1. What is a Subject Access Request (SAR)?

Section 7 of the DPA provides individuals with the right to request access to their personal data. If the individual makes a request in writing to the data controller they are entitled, subject to exemptions, to:

- Be informed by the data controller whether it or someone else on their behalf is processing that individual's personal data;
- a description of the personal data;
- the reasons for which they are being processed;
- the identity of those to whom the data are, or may be, disclosed;
- the information which constitutes personal data. It must be supplied in permanent form by way of a copy, unless this would involve disproportionate effort or the individual agrees otherwise. In such cases, other arrangements should be agreed with the requester such as allowing the individual to view the information (under supervision) on screen;
- If any of the information in the copy is not intelligible without explanation, the individual is entitled to an explanation of that information, e.g. it is in a coded form which cannot be understood without the key to the code; and
- any information as to the source of those data.

The fee for dealing with a Subject Access Request (SAR) is £10. The fee will be requested and processed by the Department. Any judicial office-holders making a SAR should not be charged the £10 fee (subject to a limit of one SAR per year, as applies to staff), nor should retired judicial office-holders who have left office within the last two years.

2. How should an SAR be dealt with?

Judicial office-holders are not expected to deal with the administration associated with SARs.

If you receive a SAR you should send it to your Knowledge and Information Liaison Officer (KILO), or if they are not known to you, to your Court or Tribunal Manager. This should be done as promptly as possible as there is a 40 calendar day time limit for dealing with the SAR. The KILO will refer the SAR to the Ministry of Justice's Data Access Compliance Unit (DACU) for further advice.

Alternatively, if you receive a SAR you should send it to DACU. If DACU accept the request as being valid, they will refer it to the Customer Feedback Team who will allocate it to a KILO.

The KILO, with advice from DACU, will draft a letter of response. Where a judicial office-holder

may be the data controller the KILO/DACU will liaise closely with them in dealing with drafting a response to the SAR.

As the data controller is responsible for ensuring that a SAR is properly dealt with according to the DPA, where you are in fact the data controller, you will also be expected to give final approval to the letter of response.

Strict timescales apply: the KILO/DACU will make sure you are aware of the relevant dates when your input is required.

3. How will the KILO/DACU deal with the SAR?

Dealing with an SAR

Your KILO/DACU will ask themselves the following questions before responding to an SAR:

1. Should a response to the SAR be provided?
2. Does the Ministry of Justice, HMCTS or a judicial office-holder hold any information relating to the subject of this request?
3. If so, does any of that information qualify as 'data' within the meaning of the DPA?
4. If so, does any of that data fall within the definition of 'personal data' or 'sensitive personal data' as set out in the DPA?
5. If so, who is the 'data controller' of this personal or sensitive personal data?
6. Does the DPA contain any exemptions which may be used so as to prevent the disclosure of personal data or sensitive personal data to the requestor?
7. Are there any other considerations?

4. Should a response to the SAR be provided?

Identification of the requester: The KILO/DACU will first confirm the identity of the person making the SAR to ensure any personal data disclosed is to the data subject and not to an impostor. If a SAR is requested from a third party purporting to act on behalf of another individual the KILO/DACU will ask to be provided with evidence that they have power to act on their behalf e.g. signed letter of consent or power of attorney.

Repeated applications: Data controllers are not obliged to comply with an identical or similar application to one already received from the same applicant unless a 'reasonable interval' has elapsed between the

two requests. A 'reasonable interval' is usually taken to equate to three months.

A response is not required if the request is not sufficiently clear to enable the data controller to find the information requested and he has made reasonable enquiries to the requester but not received the further information required.

5. Does the Ministry of Justice, HMCTS or a judicial office-holder hold any information relating to the subject of this request?

Information which is potentially within scope:There are many types of information that could contain personal data within the scope of the request. It is important to remember that this information could be held in court or tribunal documents, evidence, judgments or orders, judicial notes, judicial references, judicial appraisals, information related to judicial discipline, information related to the leadership and management functions of judicial office-holders, the Judicial Portal, any other judicial device or system, correspondence, documents related to committees and councils, or data held in e-mail systems.

It should not be assumed that information does not fall within the scope of the request because it is stored or processed by someone other than the data controller. Information held or processed by circuit secretariats, court staff, tribunal staff or private offices may fall within the scope of the request.

6. Does any of the relevant information qualify as 'data' within the meaning of the DPA?

The definition of 'data' is explained in **Annex A.**

7. Does any of that data fall within the definition of 'personal data' or 'sensitive personal data' as set out in the DPA?

The definitions of "personal data" and 'sensitive personal data' are set out in **Annex A.** It is important to remember that although personal data often forms part of a document, the right is one of access to personal data, and not necessarily to a document.

8. Who is the 'data controller' of this personal or sensitive personal data?

S1(1) DPA defines the data controller as:

> "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed"

S1(4) DPA provides that:

> "where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller"

There can be more than one data controller. For example, where there are three judicial office-holders in a constitution, each one is likely to be a data controller in his or her own right. There will also be a number of instances where both the judiciary and the Department are data controllers or act as data controllers at different stages of a given process.

Data controllers determine the purpose for and manner by which the data are processed. This is very important as it is the key factor in determining who is the data controller i.e. HMCTS or an individual judicial office-holder.

As responsibility for complying with SARs falls upon the data controller it is very important that the KILO/DACU and the judiciary take time to consider who is the data controller by examining who determines the purpose and manner by which the data is processed.

The fact that an individual judicial office-holder "processes" data will not necessarily make them a data controller in respect of it. It is only where the person determines the purpose for and manner by which the data is processed that they will be the data controller.

'Processing' is defined in s1(1) of the DPA. It should be noted that:

- Processing may be 'active'. For example recording an address on a computer system;
- Processing may also be 'passive', e.g. the mere storage of data on a manual or a computerised storage system; and
- It covers all forms of transfer and disclosure of data.

Any activity that can be done to data is likely to be within the definition of 'processing'. Whilst data processors are not under a duty to respond to SARs they must comply with the other duties and obligations in respect of processing personal data under the DPA.

9. Does the DPA contain any exemptions which may be used so as to prevent the disclosure of personal data or sensitive personal data to the requestor?

There are a number of exemptions at sections 27- 39 and Schedule 7 to the DPA. These recognise that there may be a public interest in withholding personal data sought in a SAR. The ones mostly likely to be relevant to the processing of data in the exercise of judicial functions are:

- Section 28(1): national security - This allows a data controller to withhold personal data sought under a SAR where non-disclosure is necessary 'for the purpose of safeguarding national security'.

- Section 29(1): crime and taxation - This allows a data controller to withhold personal data sought under a SAR where disclosure would be likely to prejudice the prevention or detection of crime, apprehension or prosecution of offenders, or the assessment or collection of any tax or duty of any imposition of a similar nature.

- Section 34: information available to the public by or under any enactment - This exemption applies where the data consist of information which the data controller is obliged to make available to the public by or under any enactment other than FoIA. This may include data which have been or must be published, made available for inspection, or otherwise. The exemption does not discriminate between data made available gratuitously or on payment of a fee. For example, this may apply to court transcripts if not already transcribed from a tape.

- Schedule 7, paragraph 3: judicial appointments and honours - Personal data are exempt from the requirement to comply with a SAR where it is processed for the purposes of:

  (i) Assessing any person's suitability for judicial office or the office of Queen's Counsel;

  (ii) Conferring by the Crown of any honour or dignity.

- Schedule 7, paragraph 10: legal professional privilege - This exempts personal data if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

10. Are there any other considerations?

Third Party personal data

There may be circumstances in which a data controller cannot comply with a SAR without revealing information about a third party who can be identified from that information. Under section 7(4) of the DPA, a data controller is not obliged to comply with a request unless:

- the third party has given consent to the disclosure of the information to the person making the request; or
- it is reasonable in all the circumstances to comply with the request without the consent of the third party.

It is necessary to balance the interests of both parties where the second set of circumstances arises. Regard should be had to any duty of confidentiality owed to the other individual, any steps taken by the data controller with a view to seeking the consent of the other individual, whether the other individual is capable of giving consent, and any express refusal of consent by the other individual (section 7(6)).

Where disclosure is not appropriate, this can usually be managed by editing or redacting any third party names or identifiers from the response.

Disproportionate Effort

Personal data does not have to be provided to the applicant in permanent form if the process of creating the permanent copy would involve 'disproportionate effort' (see section 8(2) of the DPA).

The Information Commissioner's view is that 'disproportionate effort' does not relate to the difficulty or workload that may be encountered in retrieving the personal data in the first place prior to providing it to the applicant. The following factors will be considered as part of any deliberations on disproportionate effort:

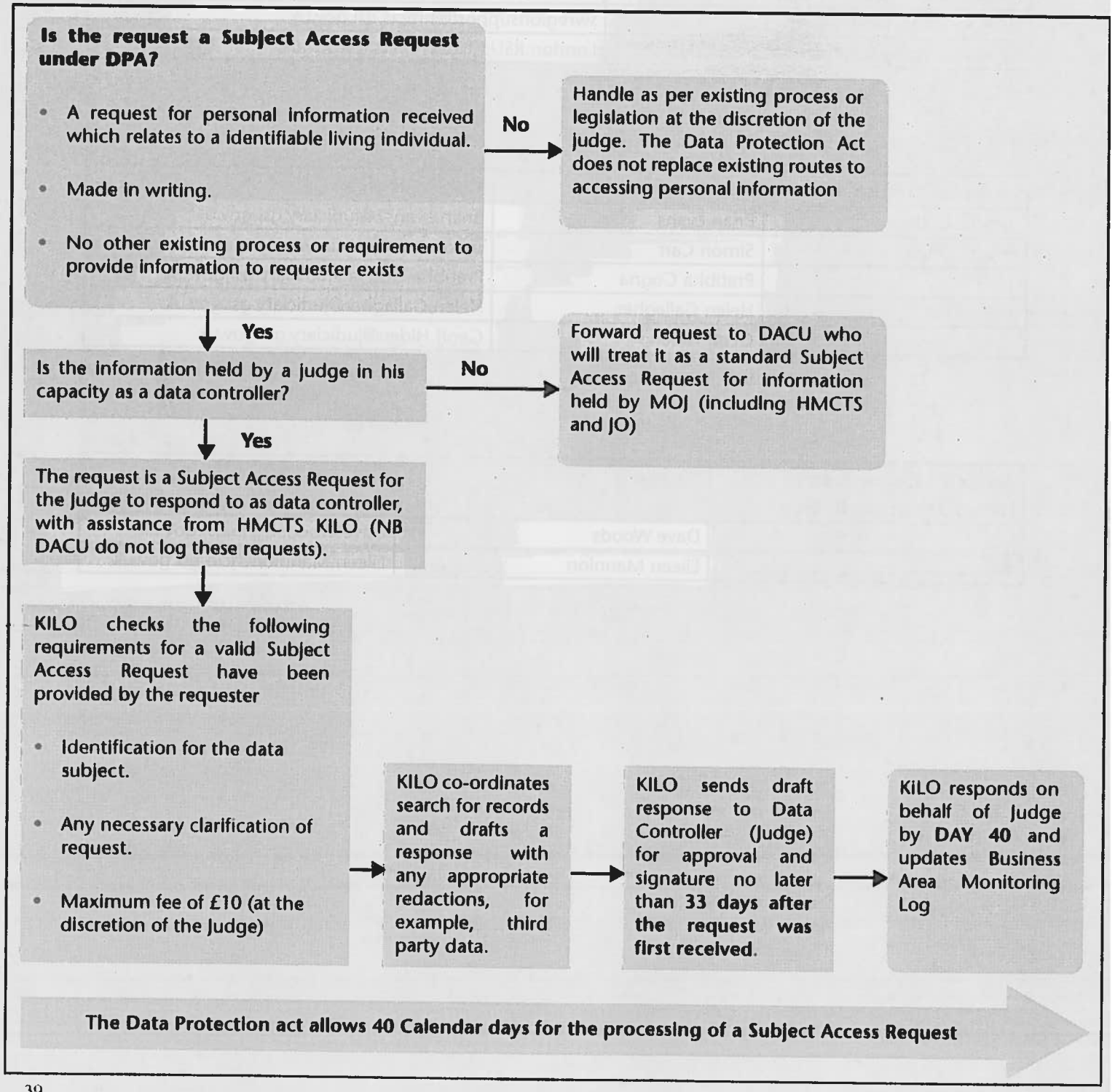
- What information/assistance has the applicant provided in identifying the personal data;
- What a reasonable person would believe to be a reasonable amount of effort – bearing in mind the £10 fee;
- How much extraction/redaction time is needed, depending on the complexity of the information and the manner in which it is stored; and
- Where the individual has not specified that they want the information, what the impact is on the individual of not having the information compared to the amount of effort in providing it.

A situation where a system is such that the information can only be viewed on screen and cannot be

exported or printed is likely to be one where the provision about 'disproportionate effort' is applicable.

Where disproportionate effort is appropriately claimed, you will be required to look for alternative means to supply access to the personal data.

11. Flow chart of the administrative process and the timelines involved



12. KILO contact details for the judiciary

HMCTS region	Contact details
HMCTS North East Region	
HMCTS North West Region	
HMCTS Midland Region	
HMCTS Wales Region	
HMCTS South Eastern Region	
HMCTS South West Region	
HMCTS London Region	

Judicial Office	Name	Contact details
Judicial College		
Private Offices		
Judicial HR		

Judicial Complaints and Investigation Office	Name	Contact details

Annex D
Regulatory Powers Available to the Information Commissioner

There are a number of powers available to the Information Commissioner to change the behaviour of organisations and individuals that collect, use and keep personal information. These powers are designed to bring about compliance with the DPA. The main powers are:

Criminal Prosecution	A sanction available where there has been a criminal breach of the DPA (section 60 Data Protection Act 1998).
Caution	An alternative to prosecution where a criminal offence under the DPA has been admitted but a caution is a more appropriate response than prosecution.
Enforcement notice	A formal notice requiring an organisation or individual to take the action specified in the notice in order to bring about compliance with the DPA and related laws. Failure to comply with a notice is a criminal offence (section 40 Data Protection Act 1998 and regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
Audit	An assessment made, with the consent of an organisation, as to whether the organisation's processing of personal data follows good practice (section 51(7) Data Protection Act 1998).
Inspection	An inspection of personal data recorded in certain European law enforcement systems in order to check compliance with the DPA (section 54A Data Protection Act 1998).
Negotiation	Not a formal regulatory power but is used widely by the Information Commissioner to bring about compliance with the DPA and related laws. Negotiated resolution can be backed by formal undertaking given by an organisation to the Commissioner.
Information notice	A notice requiring an organisation or person to supply the Commissioner with the information specified in the notice for the purpose of assessing whether the DPA or related laws have been complied with. Failure to comply with a notice is a criminal offence (sections 43 and 44 Data Protection Act 1998 and regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
Search warrant	Powers of entry and inspection, on an application to a judge, where there are reasonable grounds for suspecting an offence under the DPA has been committed or the Data Protection Principles have been contravened (section 50 and schedule 9 Data Protection Act 1998).

Section 159 order	An order requiring a credit reference agency to add a 'notice of correction' to a consumer's file (section 159 Consumer Credit Act 1974).
Application for an injunction	An injunction issued by a court under the Unfair Terms in Consumer Contract Regulations 1999 to prevent the continued use of an unfair contract term (regulation 12 Unfair Terms in Consumer Contract Regulations 1999).
Application for an enforcement order	An order issued by a court requiring a person to cease conduct harmful to consumers (section 213 Enterprises Act 2002)

The Criminal Justice and Immigration Act 2008 amended s.55 of the Data Protection Act to introduce new powers for the Information Commissioner to impose civil monetary penalties on data controllers that knowingly or recklessly commit serious contravention of the data protection principles (including security).

Further information on the Information Commissioner's powers can be found at:
http://www.ico.gov.uk/what_we_cover/data_protection/our_legal_powers.aspx

Annex E
Government Security Classification Policy

Guidance from the Senior Presiding Judge

This guidance is to ensure that judges are aware that the Government Protective Marking System has been replaced. The changes are designed to simplify the previous system; helping to ensure that information we process is correctly marked. Judges have statutory responsibilities regarding the handling of information; together with the need to preserve public confidence that sensitive matters are kept safe by them.

The previous six protective markings will no longer apply; in practice there will be little change in how we handle and protect information.

The following new system will apply from **2 April 2014:**

1. OFFICIAL - The majority of information that is created / processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

    1.1. OFFICIAL-SENSITIVE – There will be some information within OFFICIAL will be especially sensitive. This should be used **by exception** in limited circumstances where there is a **clear and justifiable requirement** to reinforce the 'need to know principle' as compromise or loss could have **damaging consequences** for an individual (or group of individuals), the Department or government more generally.

2. SECRET - This will be very sensitive information that justifies heightened protective measures to defend against determined / highly capability threats and where compromise may seriously damage military capabilities, international relations or the investigation of serious organised crime.

3. TOP SECRET - Her Majesty's Government's most sensitive information requiring the highest levels of protection from the most serious threats. Where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

It should be noted that Judges will need to apply these controls from the 2 April 2014. Further guidance is available on the intranet.

Lord Justice Gross

Senior Presiding Judge for England and Wales

Annex F
Loss of Data by the Judiciary

High Impact

Low Impact

1. Immediately inform (even if all the details are not clear):

The Senior Presiding Judge's (SPJ) or relevant Chamber President's (CP) office by telephone and email.

- **The Court/Tribunal Manager and your local judicial colleague with management responsibility i.e. Resident judge, Regional Tribunal Judge, Senior District Judge (Chief Magistrate), Bench chairmen & the police (if the data has been stolen).**

2. Senior Presiding Judge's office/Chamber President makes assessment of potential impact. Assessment may consider if the incident:

- **A sensitive case file?**
- **Was the data lost in transit /is it suspected to be in the public domain?**
- **Is it immediately evident that the case file is outside of Court premises?**
- **Is the loss likely to generate media and public interest?**
- **Will there be an impact on court proceedings?**
- **Is there a risk to personal safety or fraud?**
- **Relates to the data of over 25 individuals**
- **Is the loss likely to damage the reputation of the judiciary**

3. The SPJ's/CP's office informs (by email/phone)

Relevant Head of Division/Senior President of Tribunals/Presiding Judge/Office of the Chief Magistrate

- **The DJO Director**
- **Delivery Director**
- **Local security advisor.**

High Impact-within 1st hour

Incident form completed by judicial office holder/court or tribunal manager with assistance by SPJ/CP's office

High Impact within 24 Hrs

1.SPJ/CP's office leads initial investigation into the case and completes risk assessment according to agreed incident reporting arrangements

2. SPJ/CP's office drafts and provides a risk assessment & advice to

DJO Chief Executive and Senior President of Tribunals/Head of Division with responsibility.

Advice to include:

- Circumstances of the incident
- Press lines (in conjunction with Judicial Communications office
- Advice on the involvement of the Information Commissioner (provided by Communications & Information Directorate).
- Data access and compliance unit

3. HMCTS to advise Ministers if data loss is court information.

High Impact Day 2 +

1.SPJ/SPT's office work with all the relevant parties to investigate full circumstances and lessons learned.

2. DACU in Communications & Information Directorate, Heads of Division, Chamber President, DJO Director & press office kept up to date with all developments and conclusions.

Decision by HOD whether matter should be referred by LCJ to the JCIO in respect of courts' judiciary (or in the first instance to the Advisory Committee in relation to magistrates) as a breach of this guidance. The CP will decide if an investigation of a tribunal judge or member is necessary.

High Impact

If appropriate JCIO/ CP to advise on any further action.

Low Impact within 24 hours

Incident form completed by judicial office holder/ court manager with assistance by SPJ/CP's office

Low Impact within 24 hrs

SPJ/CP's office to provide brief summary of facts to SPT, HOD's, JCIO & DJO Director

Low Impact day 2+

HMCTS to consider whether ministers need to be advised

Low Impact

SPT/HOD to consider whether warning letter to be sent to judge

High & Low Impact

Register of actual /potential loss kept and monitored on a quarterly basis