What to do if you lose papers, or if your data security is breached

Purpose:	To guide all barristers on good practice following a breach of data or loss of papers
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Originally issued:	January 2017
Last reviewed:	January 2017
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

1. The confidentiality of clients' information could be put at risk in a number of different ways. For example:

   a) leaving papers on a train

   b) theft of a laptop, tablet or smartphone

   c) a computer or mobile device becoming infected by a virus or other malware, perhaps as a result of opening an attachment to an email or clicking on a link in a phishing email.

2. There is no single expression which would cover each of these different situations. The EU's new General Data Protection Regulation ("GDPR")[1] defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed", and for that reason the different situations mentioned above are referred to in this memo as "data breaches". "Breach" in this context refers to a breach of security, as opposed to a breach of the duty of confidentiality in rC15 of the Handbook or a breach of the Data Protection Principles set out in Schedule 1 to the Data Protection Act 1998. "Data" covers both electronic data and physical papers.

3. rC15 of the Handbook (revised January 2014) requires barristers to protect the confidentiality of a clients' affairs:

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

> *"… you must protect the confidentiality of each client's affairs, except for such disclosures as are required by law or to which your client gives informed consent"*

4. Barristers must also observe the Data Protection Principles in relation to the personal data of clients and other individuals. General guidance on what to do in the event of a data breach is provided on the Information Commissioner's ("ICO") website[2]. Much of the guidance in this document is based on the guidance from the ICO.

5. Individual barristers are almost always Data Controllers for the purposes of the Data Protection Act. Each member of Chambers normally owns the computer equipment and mobile devices which he or she uses. It is therefore the responsibility of individual members of Chambers to take appropriate precautions in relation to the security of their own equipment and communications.

6. The Seventh Data Protection Principle (7th DPP) requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This duty applies whether or not the data is in the public domain (for example a witness statement which has been read out in open court; although in such a case damage will not usually be suffered as a result of a third party accessing such a document).

7. As of December 2016, there is no general obligation to report loss of personal data to the ICO, though the ICO expects to be notified in serious cases. The ICO may impose a penalty of up to £500,000 for a breach of the DPP arising from the loss of data. Factors affecting the size of the penalty include the seriousness of the breach and the conduct of the data controller following the breach, such as whether or not the breach has been reported to the Information Commissioner's Office or the Bar Standards Board or to the data subjects affected. This will increase to 20 million Euros under the General Data Protection Directive ("GDPR"), which is planned to enter into force in May 2018. Even after the United Kingdom has left the EU it is possible that at least in the short term the Government may decide to retain the effect of the GDPR, and it would be sensible to plan on that basis. The ICO may also require undertakings as to your future conduct, for example an undertaking to encrypt a laptop computer and to keep it under lock and key when not in use.

8. Articles 33 and 34 of the GDPR will require notification of a data breach to the ICO and to data subjects in specified circumstances. These are referred to below.

9. In the event that a failure to keep information secure amounts to "serious misconduct", a barrister could be obliged to report him or herself or another barrister to the Bar Standards Board ("BSB") under rules C65.7 or C66 of the Code of Conduct. In the event of such a failure by a barrister, the barrister is obliged to take all reasonable steps to mitigate the effects, according to the guidance (gC94) under rule C65.

10. If your Chambers has an Incident Response Plan, this should be followed. A draft Incident Response Plan, which may be adapted for your or your Chambers' use, is contained in the Annex to this document.

---

[2] See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

11. The ICO's guidance states that there are four elements to a breach management plan:

a) containment and recovery

b) assessment of ongoing risk

c) notification of breach

d) evaluation and response

Containment and recovery

12. In the event of a breach affecting an individual barrister, it is necessary to consider whether Chambers needs to be informed of the breach, and if so, who should be informed. This may be covered by the Chambers IT Policy. The Bar Council's document on Information Security states that when a loss or theft occurs, Chambers, the professional client and (if appropriate) the police should be immediately informed.

13. In the event of a breach affecting Chambers as a whole, it may be necessary to take advice from an IT consultant on the steps to be taken to limit the damage caused and to prevent further damage or a repetition.

14. Where appropriate, the police, insurers and indemnity providers e.g. BMIF, should be informed.

Assessing the risks

15. It is important to consider the risks arising from the loss. There could be a big difference between the loss of one ring binder of papers and the loss of an unencrypted laptop. The assessment needs to consider the potential adverse consequences for clients, whether they are companies or individuals, and for individuals who are not clients (e.g. names and contact details in a database of a company's customers). The questions to consider include the following:

a) What type of data is involved (for example, banking details, criminal records, health records)?

b) How sensitive is the data? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details). 'Sensitive personal data' is defined in section 2 of the DPA as personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

c) If a device has been lost or stolen, are there any protections in place for the data, such as encryption?

d) What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.

e) Regardless of what has happened to the data, what could the information tell a third party about the individual? Is there a risk of identity theft? Sensitive data (e.g. trade union membership) could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information (e.g. name, address, telephone number, National Insurance number) could help a determined fraudster to build up a detailed picture of other people to exploit.

f) How many individuals are affected by the breach? It is not always the case that the bigger risks will accrue from the loss of large amounts of data but this is certainly an important determining factor in the overall risk assessment.

g) Who are the individuals whose data has been breached? Whether they are lay or professional clients or witnesses, for example, may affect the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.

h) What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and impacts on other aspects of their life?

i) Are there wider consequences to consider such as a risk to public health or loss of public confidence?

j) If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification of breaches

16. Informing Chambers has already been referred to above.

17. Reference has also been made above to informing the BSB in the event of serious misconduct.

18. At the time of writing, December 2016 (but see below in relation to the GDPR), there is no obligation to notify the ICO, and it may be unnecessary to do so in the event of a minor or low risk loss: In the event of a more serious loss, a failure to notify the ICO may be regarded as an aggravating factor when the ICO is considering whether to impose a monetary penalty. The ICO's Guidance states: "If a large number of people are affected, or there are very serious consequences, you should inform the ICO".

19. The ICO has a downloadable form which you can use for notifying a breach[3]. It requires (amongst other information) your details, information about the incident, the information at risk and remedial actions taken. The ICO has produced guidance for organisations on the information they expect to receive as part of a breach notification and

[3] https://ico.org.uk/for-organisations/report-a-breach/

on what organisations can expect from them on receipt of their notification. This guidance is available on their website[4].

20. Where appropriate, the police, insurers and/or indemnity providers such as BMIF, should be informed.

21. Where there is a significant risk of substantial damage to a client, you need to consider whether to inform your solicitors, your lay client, or opposing parties, especially where sensitive data is concerned. Reporting to the professional client is mandatory when instructed by the Government, and may also be required by contract terms.

22. Where individuals who are not clients may be affected, it is necessary to consider the risk of harm to those individuals and whether notifying them may help to reduce the risk of harm. It would rarely be necessary to notify non-clients, but if you do need to do so the following points made in the ICO's Guidance may be relevant:

a) There are a number of different ways to notify those affected, and you need to consider what method is most appropriate. Bear in mind the security of the medium as well as the urgency of the situation.

b) Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach.

c) When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.

d) Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a phone number or a web page.

23. Articles 33 and 34 of the GDPR will require notification of a data breach to the ICO and to data subjects in specified circumstances. It could be helpful to have these points in mind even before the GDPR comes into effect:

a) Notifying the ICO (GDPR Article 33):

i. In the case of a personal data breach, a data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ii. A data processor must notify the controller without undue delay after becoming aware of a personal data breach. This means that, for

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

example, clerks should inform barristers of a breach of Chambers' security as soon as possible, as they are processing information for the data controller barristers.

iii. The notification referred to in (1) above shall at least:

(1) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(3) describe the likely consequences of the personal data breach;

(4) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

iv. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

v. The data controller must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the GDPR.

b) Notifying data subjects (GDPR Article 34):

i. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the personal data breach to the data subject without undue delay.

ii. The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) above.

iii. The communication to the data subject will not be required if any of the following conditions are met:

(1) the controller has implemented appropriate technical and organisational protection measures, and those

measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(2) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in (1) is no longer likely to materialise;

(3) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

iv. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in (3) above are met.

Evaluation and response

24. After investigating the causes of the breach and taking steps to limit the damage caused, it is important to review your procedures, methods of working and configuration of IT systems and equipment to see whether they need to be improved in order to prevent a repetition. If you are reading this guidance before there has been a breach, then considering these issues may prevent a breach occurring. The following points will assist you with such a review:

a) Make sure you know what data you have and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved.

b) Think about whether there are categories of data which you do not need to retain, and delete unnecessary data.

c) Think about whether your data is being stored in places where it may not be sufficiently secure, for example on Gmail or Dropbox, and take steps to store it more securely.

d) Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks.

e) Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

f) If your Chambers already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches,

and identifying a group of people responsible for reacting to reported breaches of security.

Important Notice

This document and its annexed sample incident response plan has been prepared by the Bar Council to assist barristers on matters of IT. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it**. It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.

ANNEX

Draft Incident Response Plan[5]

1. Assess what systems have been affected

    1.1. Servers;

    1.2. Email;

    1.3. Broadband;

    1.4. local network;

    1.5. remote access;

    1.6. telephones;

    1.7. practice management system;

    1.8. word-processing and other barristers' files?;

    1.9. mobile devices or storage.

2. Inform

    2.1. Chair of IT Committee (if unavailable, notify another member of IT Committee) [if there is no IT committee, Head of Management Committee or Head of Chambers and Senior Clerk or Practice Manager;

    2.2. Helpdesk

If email is not working, use telephone;

3. Identify the means used to enable the attack to take place;

4. Assess the seriousness of the breach:

    4.1. has confidential data or personal been compromised?

    4.2. whose confidential data or personal has been compromised?

    4.3. how serious could it be if the data was disclosed to third parties?

5. Consider whether to inform

    5.1. Chair of Management Committee

    5.2. Chair of Compliance

    5.3. Head of Chambers

---

[5] See http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

5.4. Senior Practice Manager

6. Identify an internal breach response team

7. Consider whether data relating to the intrusion needs to be preserved in a forensically sound manner. If yes, obtain advice from a specialist security consultant on how this should be done (e.g. ……*insert*).

8. Prioritise restoration of systems as follows:

8.1. local network;

8.2. practice management;

8.3. barristers' data;

8.4. broadband;

8.5. email;

8.6. telephones;

8.7. remote access;

8.8. mobile devices or storage.

9. Consider whether to notify third parties, and criteria for deciding which third parties should be notified (e.g. solicitors, lay clients, factual witnesses, expert witnesses, opposing parties in litigation).

10. Consider whether to notify BSB, CJSM, ICO, Police, insurers and/or indemnity providers, if appropriate.

11. Investigate the causes of the incident, the effectiveness of Chamber's response to the incident, and the steps needed to prevent repetition (including configuration of IT facilities and amendments to policies and procedures).