Temple Court Chambers

Information Management Policy

(in relation to members of Chambers and second six pupils)

(as amended on 1st July 2022)

This Policy Document applies to barristers, including pupils when acting as data controllers.
It should be read in conjunction with the policy relating to staff, first six pupils and mini-pupils which is attached at the conclusion of this policy and to take account of its contents in the use of their own and Chambers ICT facilities and in relation to the management of information generally.

Members of Chambers are expected to put in place adequate information security measures to protect data, to protect the rights of data subjects and to fulfil their regulatory obligations as data controllers.

Introduction

1. rC15.5 of the BSB Handbook states:

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

2. It is your individual responsibility as a barrister to preserve the confidentiality of your client's affairs.

3. In the absence of specific instructions from instructing solicitors, these guidelines are intended to apply to all material received or brought into being by barristers in connection with their professional work and which contain confidential material and/or personal data to which the Data Protection legislation applies. Such information is referred to in these guidelines as "Confidential Material".

4. The use of the term "should" in these guidelines refers to good practice, of application in most situations and where any deviation will require justification according to the specific circumstances; a general practice which deviates is unlikely to be acceptable. The use of the term "must'' means that compliance is required to meet obligations under the BSB Handbook.

The receipt and handling of physical material

5. Confidential Material should not be left in a position where it might be read inadvertently by another person entering the room.

6. Confidential Material should not be read or worked on in public where it can be overlooked by members of the public.

7. Confidential Material should be stored in chambers or any other secure place to which the barrister instructed has regular access. If Confidential Material is taken out of chambers, you should try to restrict the amount taken out to what is necessary.

8. Confidential Material should be moved securely. On public transport Confidential Material should not be left unattended. If travelling by private car, where practicable, keep Confidential Material out of sight and store it as inconspicuously as possible. Confidential Material should not be left in a car unattended except where the risk of doing so is less than the risk of taking it with you. It should not be left in an unattended car overnight.

Physical security of electronic devices

9. You should also take appropriate steps to ensure the physical security of desktop computers, laptops, tablets, smartphones, PDAs, and USB sticks and other removable storage devices that contain Confidential Material.

10. In particular you should not:

    - leave devices in an unattended car overnight, and;
    - leave devices unattended in a public place (although there is no objection to leaving them in a locked court-room during adjournments).

11. Where possible, computers, tablets and smartphones used for professional purposes should not be placed so that their screens can be overlooked, especially in public places.

Laptops and other portable devices

12. Particular risks to client confidentiality arise from the loss of Confidential Material held on laptop computers, tablets, smartphones, PDAs, USB sticks and other removable storage devices. A single portable device may contain years of work that will contain very large amounts of Confidential Material. The loss of information that you are used to handling on a routine basis (such as previous convictions, commercial contracts, and medical reports) may cause considerable embarrassment to third parties as well as being a breach of the BSB Handbook and the Data Protection legislation. You should take as much care with this material as you would with your own valuables to prevent theft or loss.

13. You should consider restricting the amount of Confidential Material stored on portable devices to the minimum.

Electronic security and encryption

14. You should use appropriate security technologies suitable for the particular device or application (for example this may include anti-virus, anti-spyware and firewall software). You should be aware that malware can sit below the level of the operating system and may not be detectable by widely available anti-virus software. You should seek advice on additional protection to guard against this. Your clerks will be able to assist where necessary. Regular scans should be carried out, and the software must be kept up to date. The latest updates to the operating system software should be installed.

15. Take care to avoid infection which may result from downloading malware, for example, by clicking on links in emails or downloading attachments or programs from sources that you do not know and trust. You should be especially vigilant concerning the risk of downloading malware by visiting websites which you do not have grounds for trusting, or by clicking on links in emails or opening attachments to emails. "Phishing" emails can be fabricated to appear to have been sent by a colleague or acquaintance, so be wary of any link or attachment in an email which you were not expecting, even an email from an apparently known and trusted sender.

16. Access to computers, tablets, smartphones and other electronic devices containing Confidential Material should be protected by password:

    - You should take care to select a secure password. Passwords used to access computers or encrypted data should be sufficiently memorable that you can avoid writing them down, but not obvious or easily guessed. Long passwords are best, as a short password can be cracked more easily by hacking software. A combination of three words, using a mixture of upper case and lower case characters and at least one numeral may be easiest to remember. Default passwords (e.g. '1234', 'admin') should always be changed. It is sensible not to use the same password for all devices, services and websites and to change your password from time to time and in any event if it is disclosed to another person or discovered. You should be aware that some websites store passwords in readable text.

    - Access using biometric technologies such as a fingerprint scanner or facial recognition software are acceptable alternatives.

17. Information stored electronically should be regularly backed up, and back-up media used for Confidential Material should be locked away, if possible. Ransomware is capable of attacking back-ups stored on a back-up drive, so back-up drives should only be kept connected when backing up data. Ransomware is also capable of attacking synchronised folders, so back-up data stored in the cloud should also be recoverable from prior versions which are not stored in a synchronised folder (known as point in time recovery).

18. Computers, tablets, smartphones and other electronic devices used at home to access Confidential Material should be protected from unauthorized and unrestricted access by third parties.

19. The Information Commissioner's Office recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information. Wherever practicable therefore, Confidential Material stored on laptop computers and other portable devices (such as memory sticks, CD-ROMs, removable hard disk drives, tablets, smartphones and PDAs) should be encrypted in a reasonably secure manner, or as specified by the professional client. It may also be appropriate to encrypt data stored on desktop computers, but this may not always be practicable. Further guidance on encryption is available on the Information Commissioner's website or through Chambers IT providers (Encryption is necessary even on a password-protected laptop since the password protection can easily be bypassed by removing the hard disk drive and installing it in another computer or an external disk drive holder. Password protection may also be bypassed in other ways.) The type of encryption that is appropriate will depend on the circumstances:

    - Whole disk encryption is more satisfactory than encryption of particular folders;

    - A computer used by family members or others may in addition require encryption of specific folders, including the user profile folder, in order to prevent unauthorized access to Confidential Material by shared users or other third parties, and;

    - Barristers using folder encryption alone should satisfy themselves that this will provide a reasonable level of security. Some programs create temporary data files from which Confidential Material could be retrieved following loss or theft of the computer. These data files, and files containing emails, may also need to be encrypted.

20. It is essential to make backups of data both before and after installing encryption, since in the event of virus infection or in the event of malfunction during or after installation of the encryption program the computer may become unusable. Some defragmentation programs are incompatible with encryption programs and may result in loss of encrypted data.

21. Where a client expressly requires that removable devices or media provided by them are used, such device or media should be used in preference to your own, unless it is apparent that it is less secure. If it is apparent that the device or media is less secure, you should discuss this with your client, including, where necessary, your lay client.

Communication

22. E-mail is a potentially insecure method of communication. Appropriate steps, such as encryption during transmission, should be taken if it is considered necessary to send particularly sensitive information by e-mail and if required by your client. In such cases you should agree with your client what encryption to use.

23. You should never send the password required to decrypt an attachment in the same e-mail as the attachment since this would self-evidently defeat the purpose of encryption to avoid interception.

24. If you arrange for e-mails to be sent to your mobile telephone, smartphone or PDA, you should ensure that the device is suitably password-protected and, if appropriate, encrypted.

25. You should take care when using the 'auto complete' function that is offered by some email systems to ensure that you do not accidentally select the incorrect email address.

26. Caution is advised when using the carbon copy (cc) function and blind carbon copy (bcc) function to ensure that you are not sending data to the incorrect recipient.

27. Lists of previously used telephone numbers, fax numbers and email addresses should be kept up to date.

28. The Data Protection legislation contains restrictions on the transfer of personal data to countries outside the European Economic Area which do not provide an adequate level of security. For this reason reputable email service providers who are based in and provide email storage facilities in the European Economic Area should generally be used. If you use an email service provider based elsewhere you should check that emails will be stored in a country where the law provides sufficient safeguards in relation to data protection and that terms and conditions provide sufficient assurances in relation to data security.

29. Connecting to the internet via a wireless network presents a particular risk of interception of communication. You should take particular care when connecting via public and unencrypted access points. You should in any event refrain from making your computer detectable by others on the network. If you use a wireless network system in your home you should ensure that it is reasonably secure.

CJSM Secure Email

30. Practitioners who use CJSM secure email, in particular, criminal defence practitioners, may find it useful to refer to the 'Frequently Asked Questions' document, which can be found on the CJSM website.

Cloud Computing

31. Barristers contemplating using cloud computing services, in particular services targeted at consumers generally, should assure themselves that the service provides sufficient safeguards in relation to confidentiality, security, reliability, availability and data deletion procedures. You may wish to refer to the Bar Council's guidance on cloud computing and the ICO's guidelines on cloud computing which may also be helpful.

32. The Data Protection legislation contains restrictions on the transfer of personal data to countries outside the European Economic Area, which do not provide an adequate level of security. For this reason reputable service providers who provide storage facilities for data in the European Economic Area should generally be used. If you use a service provider based elsewhere you should check that data will only be stored in a country where the law provides sufficient safeguards in relation to data protection and that terms and conditions provide sufficient assurances in relation to data security.

33. Some cloud storage facilities state that they provide encryption, but this does not mean that files stored in the cloud are accessible only to the cloud storage service provider's customer. Some cloud storage service providers are able to gain access to the contents of encrypted files in order that they can provide access in accordance with a court order or a governmental request. Barristers using cloud storage facilities to store sensitive data should consider encrypting files themselves before uploading to the cloud, or using a cloud service provider whose software encrypts files before uploading.

Fax security

34. If you use fax, you should be aware of the Information Commissioner's guidelines, which are as follows:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.

- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

- If the fax is sensitive, ask the recipient to confirm that someone is at the fax machine and ready to receive the document, and that there is sufficient paper in the machine.

- Ring up or email to make sure the whole document has been received safely.

- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

Disposal

35. It is a requirement of the Data Protection legislation that personal data (as defined in the Data Protection legislation) should not be retained for longer than is required. However, this may be 7 years or longer for case files. Data retention, review and deletion schedules should be set up both in respect of barristers' own systems. Individual barristers will need to implement the schedules on their own systems. Individual barristers may decide to vary these schedules to meet the requirements of their own practice. The retention of precedents, pleadings, advices and documents that have been used in open court, from which personal data have been removed by anonymising, is not a breach of the requirements of the Data Protection legislation.

36. Chambers has procedures in place for the secure disposal of Confidential Material and electronic media (e.g. the cross-cut shredding of papers and CD-ROMs), and hard drives.

37. Barristers who wish to dispose of any computer or electronic media upon which Confidential Material has been stored must ensure the material is effectively destroyed or wiped using a Chambers method to put the data beyond recovery. Merely deleting the files, single-pass overwriting, or reformatting the disk is insufficient. Physical destruction or the use of specialist deletion and overwriting software is necessary.

38. Barristers whose practice includes work for Government departments or agencies will need to comply with the Attorney General's Guidelines on Information Security and Government Work.

39. The Information Commissioner's website provides detailed guidance on information security. Very substantial monetary penalties may be imposed in the event of serious contravention of the Data Protection legislation. Such contraventions may include loss of laptops, portable devices or portable storage media, where the data remains accessible to third parties. BMIF have advised that such penalties are not covered by their professional indemnity insurance. 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 when and whether or not the breach is reported to the Information Commissioner's Office. In the event that a failure to keep information secure amounts to "serious misconduct", a barrister would be obliged to report him or herself or another barrister to the Bar Standards Board under rC65.7 or rC66 of the BSB Handbook. In the event of such

a failure, a barrister is obliged to take all reasonable steps to mitigate the effects, according to the guidance (gC94) under rC65.

Information Management Policy

in relation to staff, first six pupils and mini-pupils

Information management represents a combination of:

1. Information systems used for handling data, information and knowledge e.g. library, precedents, case management, case files etc.
2. Information and Communication Technology (I.C.T.) by which is meant the tools which support our information systems represented by the variety of hardware and software (both generalist and specialist) which is available to us and the Barristers
3. Chambers systems, by which is meant operational processes and procedures for the conduct of our Chambers and which require the support of I.T while inevitably resulting in the development of Information Security (IS).
4. Information assets -being that information, data and knowledge that Chambers collects in the course of its activities, be it about staff, Barristers, its clients or other third parties with whom Chambers deals.

Our Information Management Policy and Procedures outline our approach to the identification, monitoring, and safeguarding of the above.

Chambers' Approach to Information Management
The persons with overall responsibility for the Information Management Policy is the Management Committee. This responsibility includes conducting an annual review of the policy to ensure its effectiveness.

Chambers and individual members of Chambers have introduced information management systems and information technology to meet their needs.

An Information Plan is prepared as part of the annual Chambers planning process and reviewed on an annual basis. This will consider the development of information systems & I.C.T. to support not only our current operations but Chambers' strategies and plans.

Members of Chambers, pupils and staff should recognise their individual and joint responsibility to follow relevant practices and procedures in order to maintain day-to-day excellence in managing the information entrusted to Chambers by clients and barristers, and to maintain our own information management systems.

The Purpose

The purpose of our policy is to prevent mismanagement of our information systems, assets and I.C.T. wherever possible in order to avoid or at least mitigate the following (the list is not exhaustive):

- proceedings under the General Data Protection Regulation
- the inability to provide services
- reputational and/or financial damage
- negligence claims
- breaches of confidentiality
- breaches of the BSB regulations

Register of Information Assets

Chambers carries out an audit of the principal information assets it holds on an annual basis. This information is contained in the GDPR Strategy Plan and includes the main categories of information we hold in relation to our clients and Chambers itself along with the security measures taken to protect them.

In general terms the types of document to be held in the systems are:

- Chambers' documents (leases, business plans, policies and procedures etc.)
- Client documents (documents relating to clients)
- Fee and diary documents
- Staff documents (contracts, payroll information etc.)
- Reference materials (statutory and case law materials, library materials)
- Other pupillage, mini-pupillage and lateral recruitment documents (as required)

The Information Asset Register also includes the arrangements for the safe disposal of assets once they are no longer required by Chambers or barristers.

Protection and security of information assets

Every barrister, member of staff and pupil is responsible for the protection and security of information assets entrusted to them.

Staff should at all times do their best to ensure the accuracy, relevance and sufficiency of any information in accordance with the processes and procedures relevant to their role and they will, at all times, seek to maintain the confidentiality and security of the Chambers' information assets.

Training & Awareness

Chambers provides training to all staff on all relevant aspects of Data Protection, Information Management and Information Technology.

New staff joining the Chambers will be introduced to the information management policy as part of their induction programme.

All staff will be alerted to changes in the information management policy and to changes to any processes and procedures relevant to their current role. If necessary they will receive further training or guidance in new processes and procedures.

Specific Areas of Information Management for Chambers' staff

I.C.T. System Security

Chambers is increasingly reliant on information and communication technology (I.C.T.) for the preparation and delivery of its services to barristers and clients. This increases the significance of effective computer management systems within Chambers. There are also important rules and procedures in relation to e-mail protocols and the use of the internet.

Chambers keeps under review its I.C.T. systems and as new technology is developed new policies and procedures may be introduced. The Head of Chambers and Management Committee are responsible for the management of the I.C.T. system and also to review I.C.T. requirements on an ongoing basis and to make purchases whenever appropriate. The Head Clerk is also responsible for organising on-going training on I.C.T. use for all personnel.

System Risk Management

System management is the responsibility of the Head Clerk.

Chambers has identified the following critical risks to our system:

- Fire
- Computer virus attack
- Theft
- Incompetence
- Malice

Chambers has in place the following processes, procedures and technology to eliminate, minimise or transfer the critical risks identified above:

- Virus protection system
- Management of system configurations
- Regular system backups
- Management of OS updates
- Use of a router firewall on its internet connection
- User passwords procedures
- Management of user accounts including restrictions of access and removal of users where access is no longer required
- Continual training on I.C.T. systems
- Restrictions on computer systems to prevent data being added or removed
- Physical security of Chambers premises

System Security

Chambers ensures the appropriate management and safe storage of electronic documents by restricting the access permissions to certain electronic folders as and when appropriate.

Passwords & Confidentiality

Where passwords are used, you:

- must choose and memorise a unique password - do not write it down or save it electronically anywhere. Do not use a password you use anywhere else.
- must not disclose the password to anyone else
- must not ask for another person's password
- must change the password immediately if anybody else becomes aware of it
- follow any internal instructions with regard to the changing and safeguarding of passwords.

Choice of passwords

You should take care to select a secure password. Passwords used to access computers or encrypted data should be sufficiently memorable that you can avoid writing them down, but not obvious or easily guessed. Long passwords are best, as a short password can be cracked more easily by hacking software. A combination of three words, using a mixture of upper case and lower-case characters and at least one numeral may be easiest to remember. Default passwords (e.g. '1234', 'admin') should always be changed. It is sensible not to use the same password for all devices, services and websites and to change your password from time to time and in any event if it is disclosed to another person or discovered. You should be aware that some websites store passwords in readable text.

Access using biometric technologies such as a fingerprint scanner or facial recognition software are acceptable alternatives.

Other Issues

If you anticipate that someone may need access to your confidential files in your absence you should arrange for the files to be copied to somewhere where that person can access them or arrange for a temporary password which is changed on your return.

If you are away from your computer you must lock the screen to protect against unauthorised access. It is sensible to have a default period set for the screen lock.

If you have access to data on computers, whether in the office or at home or elsewhere, you must take adequate precautions to ensure confidentiality so that

neither Chambers nor individuals are liable to prosecution as a result of loss or disclosure which might cause distress or hardship to present, former or potential employees, barristers or clients. Data should not be left in a position where it might be read inadvertently by another person entering the room. Data should not be read or worked on in public where it can be overlooked by members of the public. You may only access those parts of our computer system which you need in order to carry out your duties.

Downloading Data and Software

Chambers' employees will have access to the Chambers' systems and data. To safeguard the systems Chambers' staff will adhere to the Chambers' policy on Downloading Data and Software:

To ensure that no malicious content can be loaded onto our system, Chambers' employees should not load any data from any kind of storage device on to the Chambers system without first obtaining the consent of a Line Manager.

Examples of data storage devices are:

- Portable external hard drives
- Media player hard drives
- USB memory sticks
- DVD-RW drives
- CD and DVD disks
- Memory cards from cameras

Data storage devices which are to be copied on to the system must be formatted before use and any transfer of data to any such device must be authorised by a Line Manager.

No electronic data, however stored, should be taken off site by staff without the authority of a Line Manager or by pupils carrying out work for a barrister with the authority of that barrister.

If such authority is given and confidential data of any sort is removed from Chambers, it should be held securely and returned to Chambers as soon as possible and immediately erased from the data storage device to which it has been temporarily saved.

No software may be loaded onto computers without the express permission of a Line Manager. Software includes applications, entertainment software, games, screen savers and demonstration software.

Disks from unknown sources or from home must not be used on the system without permission and without prior checking for viruses.

Saving Documents

All documents should be saved to the appropriate folder and not to local drives or the 'my documents' folder.

Use of Personal I.C.T. equipment in Chambers

Unless specifically authorised by the Head Clerk or Management Committee personal I.C.T. equipment used by Chambers' employees must not be connected to the I.C.T. systems for any reason and to do so may be a disciplinary offence. Examples of personal I.C.T. equipment include:

- laptops
- gaming devices
- iPhones
- iPods
- digital cameras
- GPS systems
- MP3 players
- Mobile telephones/smart phones
- Laptops and mobile devices (including storage devices)

Care must be taken when taking outside Chambers laptop computers and mobile devices which are used for work. Laptops and mobile storage devices must be encrypted and must never be left unattended. In particular, they must not be left unattended in cars, whether the cars are locked or not. When travelling, these should, where practicable, be kept out of sight and stored as inconspicuously as possible. Any loss of a desktop, laptop, tablet, tablet, smartphone, or portable storage device must immediately be reported to the Head Clerk.

Accessing the System from Outside Chambers

The system has the capability for barristers, pupils and staff to access the system from home, using laptops or another external computer equipment. The principles, policies and procedures that apply to use within Chambers apply to such situations and all barristers, pupils and staff involved must be conscious of this in their work. Although Chambers has firewalls and security systems in place it is expected that anyone working on external I.C.T. must ensure that their personal equipment also has anti-virus and firewall facilities installed to prevent security risks from external access. Care should be taken when using public Wi-Fi facilities in public places (for example, coffee shops, airports, trains) as such public systems enable data easily to be accessed by unauthorised third parties. Accordingly, consideration should be given as to the use of such public Wi-Fi facilities and the risk to data as a result. It is more sensible to avoid using public Wi-Fi and to use a password protected secure mobile broadband device.

General

All active applications should be closed before logging out.

All systems should be shut down and switched off before leaving [(as should printers by the last employee to leave an area)]. Staff must ensure that their machine has correctly shut down before leaving.

You are not allowed to make any changes to the configuration or connections of the Chambers' IT system without authorisation from you’re the Management Committee.