Dere Street Barristers Information Management Policy

in relation to members of Chambers and second six pupils

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:

    10.1 leave devices in an unattended car overnight, and;

    10.2 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:

    16.1 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.

    16.2 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:

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

19.2 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;

19.3 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. In the case of service providers in the USA there is a known risk that emails could be accessed by governmental authorities or following a court order. Moreover, a non-US subsidiary of a US company may be required to disclose information which is stored outside the USA to US governmental authorities. You should therefore consider whether the information contained in your communications is of a nature which needs to be kept secure from US governmental authorities, so that US-owned email service providers should not be used.

29. Although there is presently in force an EU US Privacy Shield Agreement, that Agreement is currently under challenge before the ECJ and is in the process of being reviewed. You should therefore consider carefully whether to store data in the US in reliance on the Privacy Shield.

30. 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

31. 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

32. 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, the

ICO's guidelines on cloud computing, and the Law Society's guidance which may also be helpful.

33. 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. You should also be aware that storage facilities located outside the USA but owned by a subsidiary of a US company may be subject to US governmental surveillance. You should also be aware of the risks arising from reliance on the EU US Privacy Shield.

34. 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

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

    35.1 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.

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

    35.3 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.

    35.4 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.

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

    35.6 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

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

Dere Street Barristers 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 Head Clerk and Head of Finance and Administration. 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.

Staff moving between roles within Chambers will receive training in the information management processes and procedures relevant to their new role.

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 Clerk and Head of Finance and Administration 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 and Head of Finance and Administration are 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 and Head of Finance and Administration.

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 Head of Finance and Administration 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 or Head of Finance and Administration.

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 your Line Manager.

Data Protection

Chambers is required to comply with legislative and regulatory provisions governing the management and storage of personal information, most notably the General Data Protection Regulation (GDPR). It is the responsibility of the Head Clerk and Head of Finance and Administration to ensure that:

- All Chambers' staff are aware of their obligations under data protection law and are provided with any update as to how they are required to support Chambers in ensuring compliance; and
- Chambers is able to demonstrate its compliance with the principles relating to processing of personal data (set out in Article 5 of the GDPR).

The General Data Protection Regulation (GDPR)
The GDPR establishes a framework of rights and duties which are designed to safeguard personal data. This Chambers retains personal data about its employees and may hold data relating to barristers' cases.

The framework under the GDPR balances the legitimate needs of organisations to collect and use personal data for Chambers and other purposes, with the right of individuals to respect for the privacy of their personal details.

Personal Data
Protection of personal data and respect for individual privacy are recognised as fundamental considerations in the day to day operations of Chambers. Chambers must comply with the GDPR. 'Personal data' means data which relates to a living individual who can be identified either:

- from the data, or
- from the data and other information which is in our possession, or is likely to come into our possession, and includes any expression of opinion about the individual and any indication of our intentions or those of any other person in respect of the individual

Meaning of "Processing"
"Processing" includes obtaining, recording, holding or disclosing information or data and carrying out operations on the information or data.

All data covered by GDPR (which includes not only computer data but also personal data held within a filing system) must be:

- processed lawfully, fairly and in a transparent manner;
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- secure

Chambers is responsible for and must be able to demonstrate compliance with, the principles listed above.

In relation to these principles:

Greater protection is required for "sensitive personal data" including information held as to a person's physical or mental health, the commission of any offence and any proceedings relating to such an offence (including the outcome or sentence in such proceedings), the person's political opinions, religious or similar beliefs, sexual orientation, membership of a trade union or genetic or biometric data.

Chambers will consider:

- whether anyone has been misled in how the data has been obtained
- whether the person from whom the information was obtained has been deceived or misled as to the purpose or purposes for which the data will be processed
- whether we have informed the data subjects of our identity, the purpose or purposes for which the data are intended to be processed and anything else which we think is necessary in order to make the processing fair

We will take reasonable steps to ensure the accuracy of the data - 'reasonable' depends on the purpose of the processing.

Personal data processed for any purpose or purposes will not be kept for longer than is necessary and for that purpose data retention, review and deletion schedules are set up and implemented.

The GDPR gives data subjects a number of rights, the foremost of which is the right to have access to their personal data where permitted under the GDPR.

Data subject rights also include prevention of processing for direct marketing purposes and these rights will be considered in any marketing activities we may undertake.

We have a duty to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data or accidental loss or destruction of, or damage to, personal data. Our Information Asset Register and Risk Register takes this fact into account and appropriate policies and procedures will be maintained to protect against damage, loss or destruction of data.

We will also take steps to ensure the reliability of any employees who have access to personal data.

Data Protection and Staff Members

Chambers holds information relating to employees, pupils, mini-pupils and barristers and is a Data Controller for that data under GDPR. Chambers may process both manually and by electronic means personal and sensitive personal data for the purposes of the administration and management of Chambers' staff's employment. There may be circumstances also where individual barristers may hold such information.

Chambers may transfer part of the information held on employees to third parties where required to do so by law, including but not limited to HMRC.

Chambers may also transfer information to third parties where it forms part of the administration of the employer/employee or membership relationship. Chambers may transfer employee information to companies and organisations that carry out processing operations as Data Processors, such as payroll companies and brokers. Chambers will only do this if the arrangement:

- is made or evidenced in writing
- the data processor will act only on instruction from us; and
- the data processor agrees to comply with obligations equivalent to those imposed on Chambers by the GDPR.

Any individual whose data is held may make a “subject access request”, i.e. a request to see what data is actually held about them. All such requests should be made in writing to the Head Clerk or Head of Finance and Administration who will arrange to comply promptly with the request.

Confidentiality

The GDPR deals specifically with the processing of data whether in paper or electronic format. However, there is a natural overlap with the subject of confidentiality which is covered in other policies and with which all personnel have a responsibility to familiarise themselves.

E-Mails
Electronic mail (e-mail) is core to the operation of Chambers. However, improper use has the potential to cause loss for which Chambers can be held liable including risk of non-compliance with various statutory requirements and threats to the security of the IT system.

Guidelines relating to E-Mails

- Do not send messages from another person's computer or under a name other than your own name.
- Do not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails to those who do not have a real need to have them.
- Only forward data and information as necessary for the performance of your duties.

Appropriate Language
Care should be taken when using e-mail to use the same standards of format, content and style as would be used in a printed format. Although a different form of communication, the approach must be the same. Improper statements can give rise to personal or commercial liability. Work on the assumption that e-mail may be read by others and do not include anything in your e-mails which could cause offence or embarrass the reader or cause embarrassment to Chambers if it were to find its way into the public domain. This includes, specifically, abusive, obscene, sexist, racist, harassing or defamatory messages. If you receive such a message do not forward it on to anyone else but report it to your line manager.

Please remember that e-mail messages from Chambers have the same legal effect as a letter on ordinary note paper. Therefore, always exercise the same caution in what you say in e-mails as you would in more formal correspondence.

Addresses
Lists of previously used e-mail addresses should be kept up to date.

In the same way that Chambers exercises discretion about giving out the telephone numbers of staff members, care should be taken in giving out e-mail addresses to avoid unwanted correspondence.

Copyright
Sending copyright work by e-mail which has been copied without the consent of the rights-owner may constitute copyright infringement and should be avoided.

E-mail makes it very easy to attach materials and to cut and paste materials from other e-mail. Doing so may infringe copyright. Consideration should always be given as to whether an infringement will occur and, if so, the material should not be used.

Incoming messages
Any suspicious or offensive messages received are immediately to be referred to your line manager.

Outgoing messages
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.

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.

Consideration should be given to using password protected documents or encryption when sending e-mails containing highly confidential or sensitive data. Encryption is required when requested by the client. 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.

Under no circumstances should e-mail be used to send, receive, browse, download, or store material which may be illegal, offensive or cause embarrassment to others. This includes (without limitation) the use of the office systems to send, receive, obtain, access, download or store pornographic material, material which is racially or sexually offensive or material which could be deemed sexist, blasphemous, defamatory or abusive.

Deletion of emails
It is the responsibility of the individual to review regularly all stored messages and delete those that are no longer required in line with the Chambers data retention policy.

Out of Office Message
If a member of staff is away from his/her desk for half a day or more, the auto-office message should be set.

Email Security
Emails can bring viruses and malicious software into the Chambers' systems. As well as causing damage to those systems and interfering with service to clients and barristers, these viruses have the potential to cause the distribution of confidential information or allow unauthorised access to it. To avoid this type of incident, staff should be especially wary of opening e-mails from completely unknown, unrecognised or unexpected sources. 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. It is not always the e-mail message itself which is the carrier of a virus but the attachment that comes with it or a link contained in the e-mail. If at all suspicious, staff should not open an attachment and should seek advice. If in doubt, delete without opening.

Unsolicited Bulk E-Mail (Spam Mail)
Spam mail can be a significant problem, overloading Chambers' systems and generally being a nuisance as well as being potentially offensive, depending on the content. Dere Street's system for filtering unsolicited mail is provided by the UTM ITC Service. It is advisable to check the quarantined mail to ensure that only spam mail is captured. All Chambers' staff are responsible for reporting Spam and unsubscribing from spam mailing lists.

Personal Use

The minimal personal use by pupils and staff of the Chambers' facilities and of their own I.C.T. such as mobile phones, iPads etc. is acceptable for e-mailing using a personal e-mail account provided:

- the use is minimal and mainly out of normal working hours for example, during lunch breaks or outside core hours of work.
- the usage does not interfere with Chambers' commitments
- the usage complies with other related policies,
- personal e-mails do not contain the Chambers footer.

Continued use of our facilities for all staff is based on the understanding that this use is not abused or overused. Such abuse or overuse could be deemed an individual disciplinary matter.

Fax security

Fax is rarely used but if you do use it 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. Lists of previously used fax numbers should be kept up to date.
- 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.

Internet

Guidelines for Internet Use

Under no circumstances should internet facilities be used to send, receive, browse, download, or store material which may be illegal, offensive or cause embarrassment to others. This includes (without limitation) the use of Chambers' systems to send, receive, obtain, access, download or store pornographic material, material which is racially or sexually offensive or material which could be deemed sexist, blasphemous, defamatory or abusive.

Cutting, duplicating or copying materials from the internet may infringe copyright. Consideration should always be given as to whether an infringement will occur and if so, the material should not be used.

You should take care not to download material or access internet services that could pose a threat to the security of our systems.

You should not enter into a contract or purchase goods and services on behalf of Chambers on the Internet without express authority to do so.

Cloud computing facilities may only be used if they have been made available by Chambers for use by members of staff and pupils, or where a barrister has specifically authorised this in relation to one of their cases.

The Chambers' internet should not be used for internet membership schemes or chat rooms.

Chambers' Staff Responsibilities

Employees have a duty to report the following to their line manager;

- Suspect emails/email attachments
- Suspect web sites
- Obscene/illegal material found on a PC
- Persistent use of the internet for personal reasons
- Persistent downloading of illegal/obscene/offensive material.

Internet Security

Chambers uses tools to automatically block access to certain websites and to automatically monitor its systems to prevent security breaches. If you need to access a website that has been blocked you should contact the Head Clerk. You may be asked to explain why you need access to the blocked website.]

General Policy re Personal Use

The minimal personal use by pupils and staff of Chambers' facilities and of their own I.C.T. such as mobiles, iPads etc. is acceptable for accessing the internet provided:

- the use is minimal and mainly out of normal working hours i.e. during lunch breaks or outside core hours of work.
- the usage does not interfere with client or Chambers' commitments
- the usage complies with other related policies

Continued use of facilities for all staff is based on the understanding that this use is not abused or overused. Such abuse or overuse could be deemed an individual disciplinary matter.

Disposal of data

Personal data and confidential material must be disposed of securely.

Hard copy papers containing personal data and confidential material must be securely shredded.

Computers and electronic storage media must be securely disposed of in accordance with Chambers' procedures.

Website Management

Management of the content of the Chambers website is the ultimate responsibility of the Head Clerk. Changes to the website can only take place on his authorisation. This includes:

- ensuring content is up to date;
- approving new or revised documents for publication
- ensuring content does not infringe copyright;
- specifying conditions for downloading material;
- ensuring compliance with the Equality & Diversity Act 2010 and in doing so considering the accessibility of the site for those who are less able;
- ensuring the provision of a privacy notice explaining how any data collected from visitors will be managed.

The website will specify that, in the event of any dispute arising as a result of content posted on the website, the jurisdiction and applicable law to be invoked is that of England and Wales.

The decision to link the website with that of any other organisation and the management of the arrangements will be the responsibility of the Head Clerk. The management of such links by an external website manager will be governed by a contract between Chambers and the website providers (currently Cargo Creative). The contract will specify sites to which the website is linked; address any legal and commercial implications; specify the circumstances of accessing the linked site; include relevant disclaimers and address copyright issues.

Social Media

Introduction

The growth of the use of social media by clients is resulting in a corresponding expectation that the legal profession should also embrace it as part of its working practices. Social media activity is beneficial for engaging with clients and other professionals and can be used to allow greater access to legal information and resources. It also provides greater opportunities for professional networking and it can be used to debate, share opinions and share experiences by 'posting' or commenting in public spaces.

However, as well as understanding the benefits of using social media, it is important that there is an awareness of the potential risks involved, in particular the potential blurring of the boundaries between personal and professional use. It is important to recognise that the same ethical obligations apply to professional conduct in an online environment as apply in all other environments.

General Policy re Personal Use

The minimal personal use for social media purposes by pupils and staff of the Chambers' facilities and of their own I.C.T. such as mobiles, iPads etc. is acceptable provided:

- the use is minimal and mainly out of normal working hours, for example, during lunch breaks or outside core hours of work.
- the usage does not interfere with client or Chambers' commitments
- the usage complies with other related policies,

Continued use of our facilities for all pupils and staff is based on the understanding that this is not abused or overused. Such abuse or overuse could be deemed an individual disciplinary matter.

Application of the Social Media Policy

These rules apply to the use of social media whether:

- during office hours or otherwise
- they are accessed using the Chambers' I.C.T. facilities and equipment
- they are accessed using equipment belonging to Chambers' staff

It applies to all individuals at all levels and grades including consultants, casual and agency workers, work experience or volunteers, regardless of working arrangements.

Social Media and our Chambers

We use social media as part of our Chambers' marketing plan, raising awareness of our Chambers' services and supporting our objectives. Only staff and approved barristers who are authorised and trained to do so may participate in social media on behalf of Chambers.

The senior clerks are responsible for social media for and on behalf of Chambers. No other person is authorised to participate in social media activities without their express approval. Any questions regarding the content or application of this policy should be directed to them.

Everyone has a role to play in protecting our Chambers' reputation. If a staff member sees a posting which disparages or reflects badly on Chambers or they see a potential breach of our social media rules, this should be reported immediately to the Head Clerk.

General Rules

Posting to any social media should never occur without proper authority.

Any uncertainty or concern about the appropriateness of any posting must be discussed with the person in charge of social media.

Client confidentiality must be maintained at all times.

The confidentiality of our own strategic and commercial information must be maintained at all times.

The use of Chambers' logos, brand names, trademarks or colour schemes must be in line with our protocols.

Never register Chambers email addresses on social media sites unless such sites are being used for a Chambers activity and you have approval to register a Chambers' email address on such a site.

Any employees making use of social media for approved use should ensure they do not infringe any copyright or intellectual property rights of others. Where appropriate, sources of information posted must be accurately cited.

Social media communications that might be misconstrued in a way which is directly or indirectly detrimental to Chambers' reputation must be avoided.

Social or any other media must never be used to make any defamatory or damaging comments about Chambers, barristers, colleagues within the workplace, or those associated with Chambers, including clients.

Where social media sites are used for commercial purposes then any contacts made are regarded as Chambers' property and as such, individuals will be required to delete the details from personal social media accounts upon termination of employment.

If Chambers uses social media for the purpose of due diligence in recruitment, it will do so in accordance with data protection and equality and diversity obligations.

Security

If using any social networking site, Chambers will review site privacy settings to control, and put restrictions on, who is able to access our information. However, we are aware that by adopting privacy settings this does not necessarily mean that the information posted on social media sites will be protected, as some sites are open to the public.

Social Media and our staff

In addition to Chambers actively participating in social media, it is recognised that members of staff may do so in a personal capacity. While we would not wish to restrict personal use of social media in using it, all personnel must:

- Never use social or any other media to make any defamatory or damaging comments about Chambers, barristers, colleagues within the workplace, or those associated with Chambers, including clients.
- Understand that comments or behaviour made via social media about Chambers, barristers, work colleagues, clients, or those associated with Chambers or anyone else, which can be associated with Chambers, and which are offensive, discriminatory, or defamatory or that may result in reputational damage for Chambers and barristers, and may give rise to disciplinary action, even if the comments or behaviour are not made using Chambers' equipment or during working hours.
- Understand that if the Chambers' name is linked to the comments/behaviour, if the nature of the contents of the comment or nature of the conduct may appear to relate to the Chambers or its staff or barristers, or if the comments are about or target someone associated with Chambers, then such conduct may well be sufficient for the matter to be viewed as work related and so a disciplinary matter.
- Never use social media in a way which is a breach of any of the Chambers internal policies.
- Never register Chambers' email addresses on social media sites.
- Never disclose any Chambers' trade secrets or confidential information relating to barristers, Chambers, and/ or its employees on social media sites.
- Never disclose any work-related issue or material that could identify an individual who is a barrister, a client or work colleague, which could adversely affect Chambers, a client or our relationship with any client.
- Never suggest that any views expressed on social media are the views or opinions of Chambers or barristers.

Data Subjects' Rights and GDPR

Data Controllers now have more obligations to facilitate data subjects' rights under GDPR. These rights include:

- Right of information and access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to portability
- Right to object

Right of Information and Access

Data subjects have the right to obtain from the Data Controller - confirmation as to whether or not his/her personal data is being processed; where it is; access to the personal data and the following information:

- The purposes of processing;
- The categories of personal data concerned;
- The recipients, or categories of recipients, to whom the personal data have been, or will be disclosed, including recipients in third countries or international organisations;
- Where possible, the length of time that the personal data will be stored for, or the criteria used to determine that period;
- The existence of the right to request from the Data Controller rectification or erasure of personal data or restriction of processing or to object to such processing;
- The right to lodge a complaint with the supervisory authority;
- Where personal data is not collected from the data subject, information as to the source;
- The existence of automated decision-making, including profiling, the logic involved in such decision-making and any consequences for the data subject; and
- Where personal data is transferred to a third country or international organisation, details of any safeguards in place.

The data controller must provide a copy of the personal data being processed free of charge – reasonable charges can be made for any further copies requested.

Right to Rectification

Data subjects have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning them from the Data Controller.

Subject to the purposes for processing, data subjects have the right to have incomplete data completed, including by means of providing a supplementary statement.

Right to Erasure ('Right to be forgotten')
Data subjects have the right to obtain from a data controller the erasure of personal data concerning them, without undue delay and the controller is obliged to erase that data where one of the following grounds applies:

- The personal data is no longer necessary in relation to the purposes for which it was collected or processed;
- The data subject withdraws the consent on which the processing is based and there is no other legal ground for processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for processing;
- The personal data has been unlawfully processed;
- The personal data has to be erased for compliance with a legal obligation; or
- The personal data has been collected in relation to the offering of information society services under Article 8.1.

Where the Data Controller has made the personal data public and is obliged to erase the personal data, the data controller; taking account of available technology and the cost of implementation, must take reasonable steps to inform data controllers processing the personal data that the data subject has requested erasure. Personal data does not require to be erased where processing is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation;
- For reasons of public interest in the area of public health Article 9.2 (h) and (i) and Article 9.3;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89.1; or
- For the establishment, exercise of defence of legal claims.

Right to Restriction of Processing
Data subjects have the right to restrict a Data Controller's processing of their personal data where:

- The accuracy of the personal data is contested by the data subject. Processing can be restricted until the Data Controller has verified the accuracy of the personal data;
- The processing is unlawful but the data subject opposes erasure and requests restriction instead;
- The Data Controller no longer needs to process the personal data but the data is required by the data subject for the establishment, exercise or defence of legal claims; or
- The data subject has objected to processing pursuant to Article 21.1, pending verification whether the legitimate grounds of the controller override those of the data subject.

Right to Portability
Data subjects have the right to receive their personal data (where they have provided it to the Data Controller), in a structured, commonly used and machine-readable format and to have the data transmitted to another data controller without hindrance, where:

- Processing is based on consent; and
- Processing is carried out by automated means.

This right is dependent on the transfer between the Data Controller and the data subject being technically feasible.

The right will not apply to processing necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

This right cannot be exercised if it will adversely affect the rights and freedoms of others.

Right to Object
Data subjects have the right to object (on grounds relating to their situation) at any time to processing of their personal data which is based on:

- Necessity for the performance of a task carried out in the public interest, or in exercise of official authority vested in the Data Controller Article 6.1.e; or
- Necessity for the purposes of legitimate interests pursued by the data controller or other third party, except where this overrides the interests and fundamental freedoms of the data subject Article 6.1.f.

The Data Controller will have to stop processing the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

If personal data is processed for direct marketing purposes, data subjects can object at any time to such processing, including profiling that is related to direct marketing. Where the data subject does object, the personal data can no longer be processed for these purposes.

The right to object must be brought to the data subject's attention at the first time of communication with the data subject and should be presented clearly and separately from any other information.

Automated Processing and Profiling
Data subjects have the right to not be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them, or significantly affects them. This right will not apply if the decision:

- Is necessary for entering into, or performance of, a contract between the data subject and the Data Controller;
- Is authorised by Union or Member State law; or
- Is based on the data subject's explicit consent.

- The Data Controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, or at least the right to obtain human intervention and contest the decision.
- Decisions referred to in paragraph 2, must not be based on special categories of data (unless the exceptions in Article 9.2 apply).

Disciplinary Action

This Policy is included in the employee handbook.

Flagrant failure to follow the rules and guidelines as outlined in any part of this Policy may be a disciplinary matter and if appropriate will be dealt with under the Chambers Disciplinary Procedure.