SIX PUMP COURT

DATA PROTECTION, PRIVACY AND INFORMATION SECURITY POLICY

PARTICULARS

Policy approval date:	1 November 2023
Policy operation date:	1 November 2023
Next review date:	1 November 2025
Data Controller:	Stephen Hockman KC
Registration Number:	Z5864317
'Chambers' means	Six Pump Court Chambers, Chambers of Stephen Hockman KC and Mark Watson KC, Temple, London, EC4Y 7AR.
Data Protection Officer:	Caron Seaward
DPO barrister support:	Ian Rees Phillips and Douglas Scott

TABLE OF CONTENTS

PART ONE – Introduction 6

Introduction 6

Further Guidance 7

PART TWO – Chambers' General Policies 8

Chambers' Approach to Data Protection, Privacy and Information Security 8

Chambers' Systems and ICT security 8

Modern Desktop and Managed Devices - overview 8

Bring Your Own Device Agreement (BYOD Agreement) and Self-Managed Devices - overview 9

Barrister responsibilities for Self-Managed Devices subject to a BYOD Agreement 9

Chambers' responsibilities for Self-Managed Devices subject to a BYOD Agreement 10

Information Assets 10

Confidentiality 11

Training & Awareness 11

System Risk Management 12

System Security 12

Passwords & Confidentiality 13

Choice of Passwords 13

Downloading Data and Software 13

Saving Documents 14

Use of Personal ICT Equipment in Chambers 14

Mobile Devices (including Storage Devices) 14

Accessing the System from Outside Chambers 15

Emails 15

Principles 15

Appropriate Language 15

Addresses 16

Copyright 16

Incoming Messages 16

Outgoing Messages 16

Deletion of Emails 17

Out of Office Messages 17

Email Security 17

Unsolicited Bulk Email (Spam Mail) 18

Personal Use 18

User Privacy Relating to Email Use 18

Internet Use 18

Guidelines for Internet Use 18

Chambers Employees' Responsibilities 19

Internet Security 19

Personal Use 19
User Privacy Relating to Internet Use 20

Disposal of Data 20

Website Management 20

Social Media 21
Introduction 21
Types of Social Media 21
Application of the Social Media Policy 22
Social Media by Chambers 22
General Rules 22
Security 23
Personal Use 23
Chambers Employees Guidelines 23

Other Issues 24

Disciplinary Action 25

PART THREE – Data Protection and the UK GDPR 26

Introduction 26

Purpose 26

Scope 26

Responsibility 27

Data Protection Officer 27

UK GDPR 27
Personal Data 28
Data Controller 28
Data Processing 28
Sensitive Data 28

Data Protection Principles 29

Processing Personal Data and Sensitive Personal Data 29

Rights of the Data Subject 30

Specific Rights 31
Right of Information and Access 31
Right to Rectification 31
Right to Erasure ('Right to be Forgotten') 32
Right to Restriction of Processing 32
Right to Portability 33
Right to Object 33

Automated Processing and Profiling 34

Confidentiality and Data Sharing 34

Data Protection Impact Assessments (DPIAs) 34

DATA PROTECTION BREACHES 34

Data Protection Breach Management Plan 35
Containment and Recovery 35

Assess the Risks 35
Notification of Breaches 35
Evaluation and Response 36
Breach Reporting Procedure 36
Reporting of Data Breaches by Barristers 37
Procedure 38
Complaints 38
Penalties 38
Data Protection and Staff Members 39
Recruitment, Complaints & Grievances 39
Data Controller 39
Disciplinary Action 40
PRIVACY NOTICE – SIX PUMP COURT CHAMBERS 40
Data Controller 40
Data Collection 40
Lawful Basis for Processing 41
Use 42
Sharing 42
Transfers Outside the UK 42
Retention 42
Data Subjects' Rights 43
Accessing and Correcting Personal Data 43
Marketing Opt-Outs 43
Website Privacy Policy 43
Cookies 43
Updates 44
PART FOUR – Members' Obligations 45
Introduction 45
Legal and regulatory requirements on barristers 45
The Receipt and Handling of Physical Materials 46
Physical Security of Electronic Devices 46
Laptops and Mobile Devices 46
Electronic Security and Encryption 47
Communication 49
CJSM Secure Email 49
Cloud Computing 50
Chambers Matters 50

Data Minimisation and Disposal **51**

PART ONE – INTRODUCTION

Introduction

Chambers is an unincorporated association of self-employed barristers in independent practice.

This **Data Protection, Privacy and Information Security Policy** (this Policy) sets out the approach taken to these matters by Chambers.

This Policy must be complied with by all Chambers' employees, barristers and pupils as well as any contractor or third party with whom Chambers contracts.

The focus of this Policy is on the central systems and services provided by Chambers to Chambers' employees and barristers.

Each barrister is additionally required to be registered as a Data Controller and maintain their own complementary Data Protection, Privacy and Information Security Policy which details the specific arrangements they have in place for their practice. These individual policies can be found on the respective barrister pages of the Chambers website.

Chambers recognises the critical importance of the matters the subject of this Policy. As set out in this Policy a strict, centrally controlled and monitored approach is taken to: (a) ensure compliance with the law and regulatory requirements; (b) meet extant guidance; (c) meet legitimate client expectations, and (d) meet the conditions of Chambers' insurance cover including cyber insurance.

The use of the term "should" in this Policy 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.

Data protection, privacy and information security 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 (ICT) meaning the tools which support information systems represented by the variety of hardware and software (both generalist and specialist) which is available to Chambers and barristers.

3. Chambers' Systems meaning operational processes and procedures for the conduct of Chambers' business and which require the support of ICT while inevitably resulting in the development of Information Security requirements.

4. Information Assets meaning information, data and knowledge that Chambers collects in the course of its activities, be it about staff, barristers, their clients or other third parties with whom Chambers deals.

This Policy sets out Chambers' approach to the identification, monitoring, and safeguarding of

the above.

Further Guidance

If any person is unsure on any aspect of this Policy and/or would like further information or guidance regarding the following, they should contact the Senior Clerk and/or Heads of Chambers in the first instance:

- Chambers' approach to data protection, privacy and information security generally
- Chambers' compliance with its UK GDPR obligations as a Data Controller
- Chambers' compliance with its UK GDPR obligations as a Data Processor
- Information security
- Training, and
- Anything else relating to this Policy.

PART TWO – CHAMBERS' GENERAL POLICIES

In **Part Two** we:

Explain the approach Chambers takes to Data Protection, Privacy and Information Security. We summarise Chambers' Systems and the steps we take to ensure ICT security.

Provide information on relevant topics including the use of emails, websites and social media.

The information is important and should be understood by Chambers' employees, pupils and barristers alike.

In relation to Chambers' employees and pupils, specific instructions are also given, and rules set which must be complied with.

A failure to do so may be a breach of the respective agreements between Chambers and an employee or pupil.

Chambers' Approach to Data Protection, Privacy and Information Security

The persons with overall responsibility for this Policy are the Heads of Chambers. This responsibility includes conducting a formal review of the Policy to ensure its effectiveness no less than **every two years**.

Notwithstanding the above and in any event, as part of the Chambers' management process, information plans including the matters covered in this Policy are reviewed on an ongoing basis**.** This considers the adequacy and where necessary the development of information systems & ICT to support Chambers' current operations and strategies and plans.

Barristers, pupils and Chambers' employees 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.

Chambers' Systems and ICT security

Modern Desktop and Managed Devices - overview

Chambers provides full device management, anti-virus and device protection solutions, otherwise referred to as **Modern Desktop**, for all staff, barristers and pupils to access and utilise Chambers' IT systems and services.

The key elements of Chambers' IT systems and services are (a) Chambers' email system (b) Chambers' IT network (ethernet and wifi, in both London and Maidstone locations) (c) Chambers' Microsoft 365 package, including OneDrive and (d) Chambers' practice management system (currently 'Lex').

By default, all staff, barristers and pupils are required to enrol their device(s) to Modern Desktop in order to gain/retain access to Chambers' IT systems and services. Devices enrolled in this Modern Desktop system are formally approved by Chambers' IT supplier (currently InstantOnIt) and such devices are known as **Managed Devices**. This default requirement is imposed so as to ensure that (a) Chambers (including its barristers, staff and Heads of Chambers) complies with all relevant regulatory requirements (including UK GDPR

and DPA 2018, and applicable BSB requirements) and (b) Chambers satisfies the requirements of its relevant insurance policies, including its Cyber Security insurance policy.

Bring Your Own Device Agreement (BYOD Agreement) and Self-Managed Devices - overview

Exceptionally Chambers may allow barristers (but not staff, pupils or any other third party with whom Chambers may engage) to access and utilise Chambers' IT systems and services using devices which are not Managed Devices (hereafter **Self-Managed Devices**) but only when the barrister has entered into a prior written agreement with Chambers to ensure that equivalent security provisions are in place. Such prior agreement must be in the form prescribed by Chambers (hereafter the **Bring Your Own Device (BYOD) Agreement**).

Chambers will ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. For these reasons use of personal devices may be refused.

The purpose of this Policy and the approach taken is to prevent mismanagement of Chambers' information systems, assets and ICT wherever possible.

Barrister responsibilities for Self-Managed Devices subject to a BYOD Agreement

Barristers must take responsibility for their own device and how they use it. They must familiarise themselves with their device and its security features so that they can ensure the safety of Chambers' information and their own. Modified devices (known as jailbroken devices) that enable root access to a device must never be used.

Taking responsibility for a device includes the following:

- Invoke the relevant security features including:
- Firewall protection – this must be enabled on the device.
- Anti-virus – up to date anti-virus software must be installed and running.
- Application and operating systems must be patched, high and critical patches should be updated within 14 days.
- Passwords and PINs must be in line with Chambers' specification for Managed Devices under Modern Desktop.
- The device must be kept up to date and supported. Old and unsupported kit must be replaced.
- Ensure that the device is not used for any purpose that would be at odds with this Policy.
- Ensure that accounts are logged out of when not in use.
- Ensure that no other person accesses Chambers' data or information.

- Take all reasonable steps to prevent theft of devices and loss of data.
- Take responsibility for any software they download onto their device.
- Report the loss of any device containing Chambers' data (including email) in accordance with this Policy.
- Be aware of any Data Protection issues and ensure personal data is handled appropriately.
- Keep information confidential where appropriate.

Chambers' responsibilities for Self-Managed Devices subject to a BYOD Agreement

The Heads of Chambers in liaison with the Chambers' Management Committee are responsible for:

- Prescribing the form and content of the Chambers BYOD Agreement.
- Reviewing the BYOD requirements, which may be subject to change (and reasonable notice will be provided of such changes save in critical situations and emergencies).
- Instructing Chambers' IT suppliers to suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full IT access in the event of a breach of the BYOD Agreement or this Policy.

The Heads of Chambers or the Chambers' Management Committee:

- May approve BYOD use following receipt of a request form completed by a barrister;
- Will maintain a list of approved users, and their agreement to abide by the terms of the BYOD Agreement and this Policy when using BYOD.

Information Assets

Chambers carries out an audit of the principal information assets it holds **once a year** and reviews this Policy as required, and the main categories of information held in relation to clients and Chambers itself along with the security measures taken to protect them.

This audit is instructed and reviewed by Chambers' Management Committee.

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

- Chambers' documents (leases, business plans, policies and procedures etc.)
- Client documents (documents relating to clients, including emails, hard and electronic copy papers, billing information, contact information and marketing details)

- Client, staff, members and third-party contact details
- 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)

All information assets are disposed of in accordance with this Policy once they are no longer required by Chambers or barristers.

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

Staff will 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 will seek to maintain the confidentiality and security of the Chambers' information assets.

Confidentiality

The UK GDPR deals specifically with the processing of personal data whether in paper or electronic format, and this is covered in greater depth below. However, there is a natural overlap with the obligation of confidentiality owed by barristers under the BSB Handbook or other professional obligations, the duty of employer/employee data confidentiality owed by Chambers' employees to Chambers and by Chambers to its employees, third parties' legitimate expectation of privacy, and/or Chambers' obligation of mutual trust and confidence to employees. Accordingly, all Chambers' staff and barristers, and third parties processing data on behalf of Chambers and barristers, will process any and all data in accordance with the most stringent of any of the possible applicable obligations in order to meet any and all of the applicable duties.

Training & Awareness

Chambers provides training to all staff on all relevant aspects of data protection, privacy, information security and ICT.

New staff joining Chambers will be introduced to this 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 this 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.

Chambers makes available training to all barristers on all relevant aspects of data protection, privacy, information security and ICT.

System Risk Management

System management is the responsibility of the Heads of Chambers and the Chambers' Management Committee.

Chambers has identified the following critical risks to its systems:

- Fire
- Computer viruses and malware
- Theft
- Negligence
- Malice

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

- Virus protection system
- Endpoint Detection & Response
- Conditional Access
- Multi-factor Authentication
- Management of system configurations
- Regular system backups
- Management of OS updates
- Use of a router firewall on its internet connection
- User password procedures
- Management of user accounts including restrictions of access and removal of users where access is no longer required
- Training on ICT systems
- Restrictions on computer systems to prevent data being added or removed
- Physical security of Chambers' premises
- Chambers' continuity planning

System Security

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

Passwords & Confidentiality

When using Chambers' email and the case management software, all ICT users shall:

- Choose and memorise a strong, unique password – these are not to be written down or saved electronically anywhere unless using a password management system
- Not disclose the password to anyone else
- Not ask for another person's password
- Change their 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

All users should take care to select a secure password. Passwords used to access computers or encrypted data should be sufficiently memorable that it can be avoided from writing them down, but so that they are 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 passwords from time to time and in any event if it is disclosed to another person or discovered. Users are 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.

Downloading Data and Software

Chambers' staff will have access to the Chambers' systems and data. To safeguard the systems, Chambers' staff will adhere to the provisions of this Policy.

To ensure that no malicious content can be loaded onto Chambers' systems, Chambers' staff should not load any data from any kind of storage device on to the Chambers system without first obtaining the consent of the Senior Clerk.

Examples of data storage devices are:

- Portable external hard drives
- USB memory sticks
- DVD-RW discs

- Memory cards

Data storage devices which are to be used to copy data from the system must be formatted before use and any transfer of data to any such device must be authorised by the Senior Clerk or by the barrister Data Controller who is controlling the data in question.

No electronic data, however stored, should be taken off site by staff or non-members without the authority of the Senior Clerk, or with the authority of the barrister Data Controller who is controlling the data in question. 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 the Senior Clerk. 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 on the Chambers' case management system and not to local drives or a 'my documents' folder on a local machine.

Use of Personal ICT Equipment in Chambers

In relation to staff and pupils engaged by Chambers personal ICT equipment must be a Managed Device (as defined above) otherwise it must not be connected to Chambers' systems for any reason.

In relation to staff to do so may be a disciplinary offence.

In relation to pupils to do so may be a breach of their Training Agreement.

In relation to barristers, personal ICT equipment must be a Managed Device (as defined above) or a Self-Managed Device subject to an extant BYOD Agreement (as defined above) otherwise it must not be connected to Chambers' systems for any reason.

Examples of personal ICT equipment include:

- Laptops
- Smart phones
- Tablet computers

Mobile Devices (including Storage Devices)

Care must be taken when taking laptop computers and mobile devices which are used for work outside Chambers. Laptops and mobile storage devices, including mobile phones and tablets, 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, smartphone, or portable storage device (such as a disk or USB drive) with access to personal, sensitive or confidential data belonging to Chambers or a barrister Data Controller (including, for example, by access to a Chambers' email account) must immediately be reported to the Heads of Chambers and Senior Clerk.

Under no circumstances must a portable storage device such as a disk or USB drive containing confidential data be sent or taken out of the United Kingdom, even if encrypted.

Accessing the System from Outside Chambers

Chambers' case management and email systems have the capability for barristers, pupils and staff to access the system from home, using laptops or other 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 ICT 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 wifi 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 wifi facilities and the risk to data as a result. It is more sensible to avoid using public wifi and to use a password protected secure mobile broadband device or a virtual private network (VPN) if available.

Emails

Email is core to the operation of Chambers. 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 ICT system.

Principles

The following should be considered Chambers' general principles in the operation of its email systems:

- No user should send messages from another person's computer or under a name other than their own name.

- No user should create email congestion by sending trivial messages or unnecessarily copying emails to those who do not have a real need to have them.

- Users should only forward data and information as necessary for the performance of their duties.

Appropriate Language

Care will be taken when using email 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. All users should work on the assumption that email may be read by others and should not include anything in emails 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. Any person receiving any such message should immediately report it to the Senior Clerk or the Heads of Chambers.

Addresses

Chambers keeps lists of email addresses for employees, members, clients and third parties. These will be kept up to date and accurate.

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

Copyright

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

Email makes it very easy to attach materials and to cut and paste materials from other email. 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

All incoming messages for a barrister about that barristers' cases must be forwarded or delivered to the barrister in question. Chambers acts as a Data Processor for the barrister in question in respect of personal data contained in such emails.

Any suspicious or offensive messages received are immediately to be referred to the Senior Clerk or the Heads of Chambers.

Outgoing Messages

Users should take care when using the ‘auto complete’ function that is offered by email systems to ensure that they 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 data is not sent to the incorrect recipient. Chambers acts as a Data Processor for the barrister in question in respect of personal data contained in such emails.

Consideration will be given to using password-protected documents or encryption when sending emails containing highly confidential or sensitive data. Encryption is required when requested by the client. The password required to decrypt an attachment will never be sent in the same email as the attachment.

Under no circumstances should email 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, save unless for the purpose of a barrister's practice.

Deletion of Emails

Chambers acts as a Data Processor for barrister Data Controllers when dealing with emails relating to a barrister's cases or instructions. Barrister Data Controllers remain liable for the actions of Chambers' staff, particularly clerks, when dealing with emails relating to a barrister's case or instructions. Chambers staff will accordingly adhere to the following process when in receipt of emails relating to a barrister's case:

- Upon receipt of an email, if necessary for the barrister to see it (such as if it includes attachments containing instructions, or a query from the client, for example) the barrister will be forwarded the email. The forwarded message sent to the barrister saved in the 'sent' folder will then be deleted.

- Any attachments such as instructions or documents will be saved onto Chambers' case management system to be available to the barrister as necessary (in addition to having been sent already via email) or for future reference (for example, if the case is returned to another member of chambers)

- The email will then be moved from the staff member's inbox on the email system to a 'data processed saved' folder where it will remain for a reasonable period not less than six months for future reference, after which period it will be deleted.

For all emails which do not specifically contain data to be processed on behalf of a member of chambers as a Data Controller, these will be moved to a 'non-data processed saved' folder when the action they relate to has been satisfied, and they will remain there for a reasonable period not less than six months for future reference, after which period they will be deleted.

It is the responsibility of all users to review regularly all stored messages and delete those that are no longer required in line at all, and each member of staff will delete unnecessary emails from their email systems in accordance with the above each quarter year.

Out of Office Messages

If a member of staff is away from his/her desk for half a day or more, the auto-office message should be set and should notify an alternative staff member to contact to any person sending email to the account with the auto-office message set. The nominated alternative staff member is to also check for any emails received by the auto-office account.

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 wary of opening emails 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 email message itself which is the carrier of a virus but the attachment that comes with it or a link contained in the email. If at all suspicious, staff should not open an attachment and should seek advice. If in doubt, delete without opening.

Unsolicited Bulk Email (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. Most systems provide scope for filtering software to prevent unsolicited mail, but the danger is that if fully utilised it may block legitimate mail as well. 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 Chambers' facilities and of their own Managed Devices is acceptable for emailing using a personal email account provided:

- Use is minimal and mainly out of normal working hours for example, during lunch breaks or outside core hours of work
- Use does not interfere with Chambers' commitments and complies with other related policies
- Personal emails do not contain the Chambers' footer

Continued use of Chambers' 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.

User Privacy Relating to Email Use

On occasions, it is necessary for Chambers to monitor correspondence and communications of employees to ensure the effective operation of ICT systems and to ensure that professional standards are maintained. There might therefore be occasions when it is necessary to check email communications to or from a member of staff.

Chambers trusts employees not to misuse these facilities. However, because employees can use email for personal reasons, it may be impractical to conduct monitoring, as described above, which does not in some way impinge on the privacy of employees. Chambers for its part undertakes not to intrude to an unnecessary extent into private emails or to use/repeat/circulate any information which may come to its knowledge by way of the monitoring. However, it is generally not advisable for staff members to send, receive or forward private emails at work which they would not want a third party to read.

Internet Use

Guidelines for Internet Use

Under no circumstances, save further to the requirements of a barrister's particular practice, 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.

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

Users 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.

Chambers Employees' Responsibilities

Employees have a duty to report the following to the Senior Clerk or the Heads of Chambers:

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

Internet Security

Chambers and its internet service provider uses tools to automatically monitor access to certain websites and to automatically protect its systems to prevent security breaches. This may include blocking websites.

Personal Use

The minimal personal use by pupils and staff of Chambers' facilities and of their own Managed Devices 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.

User Privacy Relating to Internet Use

On occasions it is necessary for Chambers to monitor correspondence and communications to ensure the effective operation of ICT systems and to ensure that professional standards are maintained. There might therefore be occasions when it is necessary to check internet communications to or from a member of staff.

Chambers trusts employees not to misuse these facilities. However, because employees are allowed to use internet for personal reasons, it may be impractical to conduct monitoring as described above, which does not in some way impinge on the privacy of employees. Chambers for its part undertakes not to intrude to an unnecessary extent into private internet use or to use/repeat/circulate any information which may come to its knowledge by way of the monitoring. However, it is generally not advisable for any user to access sites at work which they would not want a third party to be aware of.

Disposal of Data

Chambers has a contract with a third-party service provider to ensure that hard copy papers can be confidentially and securely shredded. Chambers has large bins for such papers and will ensure that all staff place any papers with any confidential or personal data on them into these bins, and that no such papers will go into the general waste to be disposed of.

Personal data and confidential material taken from the internet or received via email must be disposed of by deleting the same from Chambers' systems when it is no longer required. All staff using Chambers' hardware must regularly delete any documents taken from the internet or which were received via email which are no longer required.

All computer hardware and electronic storage media are always securely disposed of by a third-party services provider when no longer in use.

Website Management

Management of the content of the Chambers website is the responsibility of Chambers' Management Committee, the Senior Clerk and the DPO. Changes to the website can only take place on their 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 Chambers' DPO. The management of such links by an external website manager will be governed by a contract between Chambers and the website manager. 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.

Chambers' website will host a copy of this Policy and will accordingly satisfy Articles 13 and 14 of the UK GDPR in respect of privacy notices for data subjects.

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.

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. Chambers recognises that the same ethical obligations apply to professional conduct in an online environment as apply in all other environments.

Types of Social Media

The following types of social media channels amount to social media for the purpose of this Policy. These include:

- Forums and comment spaces on information-based websites
- Social networking websites such as Facebook, LinkedIn etc.
- Video and photo sharing websites such as Flickr and YouTube
- Blogs, including corporate and personal blogs
- Micro-blogging sites such as Twitter/X
- Forums and discussion boards such as Google Groups
- Online wikis that allow collaborative information sharing such as Wikipedia

- Any other websites that allow individual users or companies to use simple publishing tools.

Application of the Social Media Policy

These rules apply to the use of social media when accessed:

- During office hours or otherwise
- Using Chambers' ICT facilities and equipment, or
- Using equipment belonging to Chambers' staff using Chambers' wifi network or internet service

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 by Chambers

Chambers uses social media as part of its marketing plan, raising awareness of Chambers' services and supporting its objectives. Its continued use will be regularly reviewed. Only staff and approved barristers who are authorised and trained to do so may participate in social media on behalf of Chambers.

Chambers' Management Committee, the Senior Clerk and the DPO are responsible for social media for and on behalf of Chambers. No other person is authorised to participate in social media activities without express prior approval. Any questions regarding the content or application of this Policy should be directed to them.

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

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 Chambers' 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 Chambers' use of them.

Chambers email addresses should not be used for social media sites unless such sites are being used for a Chambers activity.

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 by employees or staff 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 Chambers' information. However, Chambers is 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.

Personal Use

The minimal personal use for social media purposes by pupils and staff of Chambers' facilities and of their own Managed Devices is acceptable provided:

- Use is minimal and mainly out of normal working hours, for example, during lunch breaks or outside core hours of work.

- Use does not interfere with client or Chambers' commitments and complies with other related policies

Continued use of Chambers' 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.

Chambers Employees Guidelines

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

Other Issues

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

If any user is away from his or her computer for more than a short period, they must lock the screen to protect against unauthorised access, and all staff will have a default period set for the screen lock to switch on automatically if the computer is not used for a time.

If any user has access to data controlled by Chambers on computers, whether in the office or at home or elsewhere, they must take adequate precautions to ensure confidentiality so that neither Chambers nor individuals are liable to prosecution or sanction 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. Users may only access those parts of Chambers' computer system which they need in order to carry out their duties. Staff are aware that Chambers processes data for barristers as a Data Processor and is responsible to those members as the relevant Data Controller when it does so.

All active applications should be closed before logging out. All systems should be shut down

and switched off before leaving. Staff must ensure that their machine has correctly shut down before leaving.

Users are not allowed to make any changes to the configuration or connections of the Chambers' ICT system. Exceptionally, and if such a need arises, you must first consult with the Senior Clerk or the Heads of Chambers.

Chambers is not a payment card industry (a PCI) in that it does not process all types of payment cards during its undertaking and consequently the regulations pertaining to PCI's do not apply to Chambers.

Chambers has formal payment procedures in place in relation to each of its bank accounts relating to the conduct of its undertaking. No change may be made to the bank details of any person receiving money from Chambers or first payment made to any person without prior independent verification and authorisation by the Senior Clerk and/or Heads of Chambers as appropriate.

Disciplinary Action

Part Two of this Policy makes up part of the Code of Conduct for all Chambers' employees. Failure to follow the rules and guidance 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.

A member of staff may be required to remove postings which are deemed to be a breach of this Policy and failure to comply with such requests may in itself be deemed a disciplinary issue.

Failure on the part of a barrister to follow relevant and applicable rules and guidance as outlined in any part of this Policy might amount to cause for Chambers to consider action against that member under its Constitution.

PART THREE – DATA PROTECTION AND THE UK GDPR

In **Part Three** we set out how Chambers complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The procedure to follow in the event of a data breach is explained.

Chambers' formal Privacy Notice is provided.

This Part is applicable to Chambers' employees, pupils, consultants and any third party providing services.

It is also relevant to barrister members who should understand the content and follow the procedures relevant to them.

Introduction

Chambers is required to comply with the law governing the management and storage of personal data, which is set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Chambers is a registered Data Controller in the identity of the Head of Chambers in accordance with its Constitution.

Chambers acts as a Data Processor for members when processing personal data under the control of individual barristers, for example by facilitating the instruction of barristers by solicitors and other clients, by Chambers' clerks forwarding emails from outside Chambers to barristers, and by Chambers' fees system billing clients on behalf of barristers etc.

It is the responsibility of the Heads of Chambers to ensure that:

- All Chambers' staff are aware of their obligations under data protection law and are provided with training 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 under the UK GDPR.

For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of Chambers.

Compliance with the UK GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). Chambers is accountable to the ICO for its data protection compliance.

Purpose

This Policy aims to protect and promote the data protection rights of individuals and of Chambers, by informing members and everyone working for and with Chambers, of their data protection obligations and of Chambers procedures that must be followed in order to ensure compliance with the UK GDPR.

Scope

This Policy applies to all Chambers' employees, consultants and any third party to whom this Policy has been communicated.

It is also relevant to barrister members who should understand the content and follow the procedures relevant to them.

This Policy covers all personal data and special categories of personal data, whether processed electronically or on hard copy files.

Responsibility

The Heads of Chambers in liaison with the Chambers' Management Committee and Chambers' DPO is responsible for monitoring Chambers' compliance with this Policy.

Everyone in Chambers (and any third party to whom this Policy applies) is responsible for ensuring that they comply with this Policy. Failure to do so may result in disciplinary action.

Data Protection Officer

The DPO's responsibilities include:

- Arranging periodic data protection training for all staff which is appropriate to them
- Arranging and making available to barristers data protection training which is appropriate to them
- Acting as a point of contact for all colleagues, staff and barristers on data protection matters
- Monitoring Chambers' compliance with its data protection policy and procedures
- Promoting a culture of data protection awareness
- Assisting with investigations into data protection breaches and helping Chambers to learn from them
- Advising on Data Protection Impact Assessment, and
- Liaising with the relevant supervisory authorities as necessary (i.e. the ICO in the UK)

The DPO is supported by appointed barristers within Chambers and also works in liaison with the Heads of Chambers and Chambers' Management Committee.

UK GDPR

The UK GDPR is designed to protect individuals and personal data about them which is held and processed by Chambers or other individuals.

The UK GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal Data

Personal data means any information relating to an identified and identifiable natural person ('a data subject')

This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; address; telephone number; email; ID number; location data; online identifiers etc. It also includes information that identifies the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

For Chambers' purposes, barristers' clients and Chambers' staff are data subjects and other individual third parties are also likely to be data subjects where Chambers holds or processes personal data about them.

Data Controller

Data Controller means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the Data Controller is the individual, organisation or other body that decides how personal data will be collected and used.

For Chambers' purposes, Chambers is a Data Controller for certain categories of data.

Data Processing

Data processing means any operation which is performed on personal data such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

For Chambers' purposes, everything that Chambers does with barristers' client information (and personal information of third parties) is 'processing' as defined by the UK GDPR. This processing will often be in the capacity as a Data Processor on behalf of a barrister as a Data Controller, but Chambers is a Data Controller for data such as collated lists of clients of all Chambers' members, lists of emails for marketing purposes on a Chambers-wide basis and of personal data held for billing barristers' clients.

Sensitive Data

Special categories of personal data apply to sensitive personal data revealing a data subject's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic data or biometric data uniquely identifying a natural person, or

- Data concerning health or data concerning a natural person's sex life or sexual orientation

Data relating to criminal convictions and offences is not included within the special categories. However, there are additional provisions for processing this type of data under Article 10 UK GDPR.

Data Protection Principles

The UK GDPR is based around 8 principles which are the starting point to ensure compliance with the UK GDPR. Everybody working in for and with Chambers must adhere to these principles in performing their day-to-day duties. The principles require Chambers to ensure that all personal data and sensitive personal data are:

(a) Processed lawfully, fairly and in a transparent manner in relation to the subject ('lawfulness, fairness and transparency')

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate (having regard to the purposes for which they are processed) are erased or rectified without delay ('accuracy')

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('storage limitation')

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

(g) Chambers must be able to demonstrate its compliance with (a) – (f) above ('accountability').

Processing Personal Data and Sensitive Personal Data

Chambers will process all personal data in a manner that is compliant with the UK GDPR, and will in each case:

- Have legitimate grounds for collecting and using the personal data

- Not use the data in ways that have unjustified adverse effects on the individuals concerned

- Be transparent about how it intends to use the data, and publish an appropriate privacy notice when collecting personal data

- Handle people's personal data only in ways they would reasonably expect, and
- Make sure it does not do anything unlawful with the data.

Chambers will ensure that it is aware of the difference between personal data and special categories of personal data and ensure that both types of data are processed in accordance with the UK GDPR.

The conditions for processing special categories of personal data that are most relevant to Chambers are:

- Explicit consent from the data subject;
- The processing is at the instruction of a barrister who is the Data Controller of that sensitive personal data;
- The processing is necessary for the purposes of carrying out Chambers' obligations in respect of employment, social security and social protection law;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

If any person has any concerns about processing personal data, they should contact Chambers' DPO, who will be happy to discuss matters.

Rights of the Data Subject

The UK GDPR gives rights to individuals in respect of the personal data that any organisations hold about them. Everybody working for Chambers will be familiar with these rights and adhere to Chambers' procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy
- Right to rectification of any inaccurate personal data
- Right to erasure of personal data held about them (in certain circumstances)
- Right to restriction on the use of personal data held about them (in certain circumstances)
- Right to portability – right to receive data processed by automated means and have it transferred to another Data Controller

- Right to object to the processing of their personal data.

If anybody within Chambers receives a request from a data subject (a client or other third party concerning whom it holds personal data) to exercise any of these rights in relation to personal data controlled by Chambers, the request must be referred to the Heads of Chambers and Senior Clerk immediately.

Chambers only has one month to respond to a request from a data subject relating to personal data.

Specific Rights

Right of Information and Access

Data subjects have the right to obtain information about, and access to data held by, a Data Controller, including confirmation as to whether or not his / her personal data is being processed, where it is, access to it, 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

Chambers must provide a copy of the personal data being processed free of charge save that 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

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 Processors 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
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or
- For the establishment, exercise or 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 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.

Confidentiality and Data Sharing

Chambers must ensure that it only shares personal information with other individuals or organisations where it is permitted to do so in accordance with the UK GDPR.

Chambers will attempt to ensure it has the client's (or other data subject's) consent before sharing their personal data, although this will not be possible in all circumstances, for example if the disclosure is required by law.

Any further questions around data sharing should be directed to the DPO.

Data Protection Impact Assessments (DPIAs)

DPIAs are required to identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks, when introducing, or making significant changes to, systems or projects involving the processing of personal data.

In simpler terms, this means thinking about whether Chambers is likely to breach the UK GDPR and what the consequences might be, if Chambers uses personal data in a particular way. It is also about deciding whether there is anything that Chambers can do to stop or, at least or minimise the chances of any of the potential problems identified, from happening.

DPIAs will be undertaken **once a year** by the DPO in liaison with Chambers' Management Committee.

DATA PROTECTION BREACHES

A data protection breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*

transmitted, stored or otherwise processed".

Everybody working in, for and with Chambers has a duty in respect of any actual or suspected breach of data protection in respect of data under the control of Chambers to report without delay to the Senior Clerk and the Heads of Chambers.

Note that if the data breach occurs when processing personal data under the control of a barrister as a Data Controller, then the responsibility for dealing with that breach lies with the barrister.

Any person employed by or acting for Chambers who is processing data for a barrister as a Data Controller will report any actual or suspected breach of data protection of personal data under their control immediately to that barrister and the Senior Clerk so that the necessary assistance may be provided. The Senior Clerk will report the matter to the Heads of Chambers.

Data Protection Breach Management Plan

There are four key steps to the Chambers' data protection breach management plan:

- Containment and recovery
- Assessment and ongoing risk
- Notification of breach
- Evaluation and response

Containment and Recovery

The reporting person must:

- Take steps to recover any lost data and limit the damage that the breach can cause where possible

The Senior Clerk and, where appropriate, the Heads of Chambers in liaison with the reporting person will:

- Decide who will lead the investigation into the breach, and
- Find out who needs to be aware of the breach and tell those persons what they are expected to do (if anything) to assist in the containment and recovery of the breach

Assess the Risks

The person leading the investigation must assess the potential adverse consequences of the breach for the data subject individuals concerned, the potential severity or scale of the breach and the likelihood of adverse consequences occurring.

Notification of Breaches

Chambers has a duty to report all data protection breaches that are likely to result in a risk to

the rights and freedoms of individuals to the ICO.

The Senior Clerk and the Heads of Chambers are responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it.

If instructed to do so by the Senior Clerk and/or the Heads of Chambers, the DPO will report the breach to the ICO in accordance with the reporting methods set by the ICO.

Where deemed appropriate, the individuals affected by the data protection breach must also be informed. The investigating person must provide individuals with specific and clear information about what has happened and what is being done to address the breach. Advice should also be offered on any steps that the affected individuals can take to protect themselves. The individuals must be given contact details should they require further information or help.

Considerations must also be made as to whether any other third parties should be notified, including, for example., the police, insurers, professional bodies, banks etc.

Evaluation and Response

Chambers' response to the data protection breach will then be evaluated. It will always be important to establish whether the breach was caused by an isolated incident or is part of a wider systemic issue so that Chambers can try to prevent the same or a similar breach from occurring in the future. Any lessons learned should be shared across Chambers as appropriate by communicating the details to the relevant members and staff of Chambers, including so that members as Data Controllers can implement any changes that might be appropriate to their own data protection policies and practice.

Chambers' Management Committee in liaison with the DPO will review all records of data breaches periodically to establish any trends requiring further attention.

There is a central record of all data protection breaches that occur.

The DPO is responsible for maintaining the data protection breach and suspected breach register.

Breach Reporting Procedure

Chambers is responsible for ensuring that personal data processed by it is not:

- Accessed without authority
- Processed unlawfully
- Lost
- Destroyed, or
- Damaged

Chambers is aware that things may go wrong, and it might fail to maintain one or more of its data protection responsibilities. If this does happen, it is essential that steps are taken to try to put things right. However, it can do this only if it knows that there has been a problem. Accordingly, everybody within Chambers, including barristers, staff, consultants, service providers, pupils and mini-pupils, has a duty to report any actual or suspected data breach by Chambers as a Data Controller or Data Processor, regardless of whether they have discovered the breaches or have caused them.

Data protection breaches can happen for a wide range of reasons, including:

- Human error
- Cyber-attacks
- Loss or theft of devices, equipment or hard copy papers on which personal data is stored
- Inadequate or inappropriate access controls
- Deceit, and
- Disasters at Chambers' premises, for example, fire or flood

If any person is unsure whether a particular circumstance or incident constitutes a data protection breach, the matter should be referred urgently to the Senior Clerk or the Heads of Chambers for guidance.

ICO Guidance provides that if a source of data is lost or stolen, but that the risk of personal data actually being released is unlikely, such as an encrypted and password-protected laptop being lost, this may not amount to a data breach, but all persons should still report any such potential breach for guidance and for a decision to be made as to whether the potential breach should be reported to the ICO or not.

All personal data breaches involving data subjects who are a member of, employed or otherwise attached to Chambers, such as Chambers' staff, pupils or members, must be reported to the Senior Clerk and the Heads of Chambers immediately upon discovery.

Reporting of Data Breaches by Barristers

As Data Controllers, barristers are under no regulatory obligation to report a breach by them or a Data Processor under their control to Chambers and are responsible individually for compliance with the notification and reporting obligations of the UK GDPR. Nonetheless, Chambers recognises the role undertaken by Chambers as a Data Processor and acknowledges an obligation to support Data Controllers in those cases where it is appropriate to do so. In the case of a data breach caused by a member of Chambers as a Data Controller, the best practice is for the barrister member to report the breach to the Senior Clerk and the Heads of Chambers as appropriate. Chambers will support any barristers reporting and managing data breaches and a coordinated approach can be taken.

Procedure

Reports should be made by email. When making a report, the person reporting must detail:

- The nature of the suspected breach (i.e. whether there has been a theft, loss, destruction, accidental disclosure etc.)
- The nature of the data involved (i.e. whether it is sensitive, personal or commercial etc.)
- The scope or extent of the breach (i.e. whether it relates to one data subject or several people etc.)
- A description of the events leading up to the breach
- The names of any Chambers' staff, members and/or other third parties involved
- The time and date the breach occurred
- The location or suspected location of the breach, and
- Any other relevant information.

Breaches will be reported to the ICO by agreement either by the barrister as Data Controller or by Chambers without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless it has been demonstrated that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Chambers will maintain a central register of the details of any data protection breaches reported.

Complaints

Complaints relating to breaches of the UK GDPR and/ or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to the Senior Clerk and the Heads of Chambers without delay.

Penalties

Everybody working for Chambers understands the implications for Chambers if it fails to meet its data protection obligations. Failure to comply could result in:

- Criminal and civil action
- Fines and damages or other regulatory action
- Personal accountability and liability
- Suspension / withdrawal of the right to process personal data by the ICO
- Loss of confidence in the integrity of Chambers' systems and procedures, or

- Irreparable damage to Chambers' reputation.

Chambers could be fined up to 4% of the total worldwide annual turnover of the preceding financial year.

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 UK 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 as Data Processors for Chambers. Chambers holds and processes such data on the basis of its legitimate interest or operating as an employer in the context of being a barristers' chambers.

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 Chambers; and
- Chambers is satisfied that that the Data Processor will comply with obligations equivalent to those imposed on Chambers by the UK 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 Senior Clerk and the Heads of Chambers who will arrange to comply promptly with the request.

Recruitment, Complaints & Grievances

Chambers' employer responsibilities will be carried out in accordance with all its UK GDPR and data protection obligations. The substantive responsibilities are set out elsewhere in Chambers' policies and/or Handbook.

When carrying out obligations on behalf of Chambers in respect of Chambers' employer responsibilities (such as, for example, in interviewing candidates for employment) or in other duties on behalf of Chambers (such as pupillage panels), members are Data Processors on behalf of Chambers as Data Controller. In all such cases Chambers will control the personal data members process and will do so in accordance with this Policy.

Data Controller

Chambers is registered with the ICO as a Data Controller for the personal data that it holds.

Disciplinary Action

Part Three of this Policy makes up part of the Code of Conduct for all Chambers' employees. 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.

A failure to comply with the UK GDPR obligations by a barrister member of Chambers, whether as a Data Controller or as a Data Processor, might amount to cause for Chambers to consider action against that member under its Constitution.

PRIVACY NOTICE – SIX PUMP COURT CHAMBERS

This is a privacy notice in accordance with Articles 13 and 14 of the UK GDPR.

Chambers need to collect and hold personal information in order to provide its services via its members. It will take all possible steps to protect all personal information. This Privacy Notice describes the information it collects about data subjects, how it is used and shared, and the subjects' rights regarding it.

Data Controller

Chambers is registered with the ICO as a Data Controller for the personal data that it holds and process as a barrister's chambers. It is registered in the identity of a Head of Chambers, Stephen Hockman KC. Its registered address is Six Pump Court Chambers, The Chambers of Stephen Hockman KC and Mark Watson KC, 6 Pump Court, Temple, London, EC4Y 7AR and its registration number is Z5864317.

Data Collection

All the information that Chambers holds about data subjects is provided to or gathered by it in the course of its business.

Chambers collects and process both personal data and special categories of personal data as defined in the UK GDPR. This includes:

- Names
- Emails
- Phone numbers
- Addresses
- Payment or bank details
- Dates of birth
- Location details

- Device IP addresses

Lawful Basis for Processing

The UK GDPR requires all organisations that process personal data to have a lawful basis for doing so. The lawful bases identified in the UK GDPR are:

- Consent of the data subject
- Performance of a contract with the data subject or to take steps to enter into a contract
- Compliance with a legal obligation
- To protect the vital interests of a data subject or another person
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The legitimate interests of Chambers, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Examples of legitimate interests include:

- Where the data subject is a client or in the service of the controller;
- Transmission within a group of undertakings for internal administrative purposes;
- Processing necessary to ensure network and information security, including preventing unauthorised access;
- Processing for direct marketing purposes, or to prevent fraud; and
- Reporting possible criminal acts or threats to public security.

Chambers' lawful bases are variously consent, performance of a contract, compliance with a legal obligation, and Chambers' legitimate interests.

Chambers processes personal data via consent given by data subjects when they contact Chambers directly via email, phone or post and contacting Chambers with a view to instructing a member of Chambers will establish consent to process any personal data communicated by that data subject, or where the data subject is employed or contracted by Chambers, or is a barrister or associate member of Chambers.

Chambers alternatively processes personal data via contract, namely contracts entered into by it and third parties such as staff members and other employees, service providers and contractors.

Chambers alternatively processes personal data via the requirement to comply with legal obligations, including but not limited to legal services regulation, health and safety at work, employment legislation, occupier's liability obligations etc.

Chambers alternatively processes personal data via its own legitimate interests, namely the operation of a barristers' chambers and the facilitation of its members' practices.

Use

Chambers uses personal data to:

- Facilitate the provision of legal advice and representation by its barrister members
- Assist in training pupils and mini-pupils
- Communicate with data subjects about news, updates and events
- Carry out its statutory obligations
- Employ its staff and enter into contracts with third parties

Chambers does not use automated decision-making in the processing of personal data.

Sharing

Chambers may share personal data with:

- Barrister members
- The barristers, clerks or staff of other chambers
- Solicitors instructing barrister members
- Pupils or mini pupils in training
- Chambers management and staff who provide administrative services
- The Bar Standards Board or other regulatory body or legal advisors in the event of a dispute or other legal matter
- Law enforcement officials, government authorities, or other third parties to meet Chambers' legal obligations
- Service providers carrying out services for Chambers, such as ICT or internet service providers
- Any other party where Chambers ask a data subject and the data subject consents to the sharing

Transfers Outside the UK

Chambers does not transfer any personal data to third countries or international organisations.

Retention

Chambers retains personal data while it remains current and necessary to do so unless a data subject asks it to delete it. Chambers holds such data for an appropriate period depending on the nature of the data involved, and will usually retain this for up to **15 years**. It will delete or anonymise data subjects' information at their request unless:

- There is an unresolved issue, such as claim or dispute
- Chambers are legally required not to do so, or
- There are overriding legitimate business interests, including but not limited to fraud prevention and protecting customers' safety and security.

Data Subjects' Rights

The UK GDPR gives data subjects specific rights around their personal data. For example, they have to be informed about the information Chambers' holds and what it uses it for, they can ask for a copy of the personal information it holds about them, they can ask Chambers to correct any inaccuracies with the personal data it holds, they can ask Chambers to stop sending them direct mail, or emails, or in some circumstances ask Chambers to stop processing their details. Finally, if Chambers does something irregular or improper with their personal data they can seek compensation for any distress caused or loss incurred. Data subjects can find out more information from the ICO's website and this is the organisation that data subjects can complain to if they are unhappy with how Chambers has dealt with them.

Accessing and Correcting Personal Data

Data subjects may request access to, correction of, or a copy of their information by contacting the Senior Clerk at Richard.Constable@6pumpcourt.co.uk.

Marketing Opt-Outs

Data subjects may opt out of receiving emails and other messages from Chambers by following the instructions in marketing messages.

Website Privacy Policy

Through the use of Google Analytics, Chambers may collect, store and use information about the device used to access Chambers', including IP address, geographical location, browser type, referral source, length of visit and number of page views.

Cookies

Cookies are small text files that are stored on your browser or device by websites, apps, online media, and advertisements. The Chambers website uses cookies to:

- Validate users
- Remember user preferences and settings
- Determine frequency of accessing our content

- Measure the effectiveness of advertising campaigns, and
- Analyse site visits and trends

Chambers' website may use both "session" cookies and "persistent" cookies on the website to respectively keep track of users whilst they navigate the website; and to enable the website to recognise users when they visit. Google Analytics generates statistical and other information about website use by means of cookies, which are stored on users' computers. The information generated relating to Chambers' website is used to create reports about the use of the website. Google will have access to and store this information. Under no circumstances is information obtained this way made available to third parties

Session cookies will be deleted from users' computers when the relevant browser is closed. Persistent cookies will remain stored on users' computers until deleted, or until they reach a specified expiry date.

Most browsers allow users to refuse to accept cookies and users of Chambers' website who wish to opt out of Chambers using cookies in the manner described should accordingly refuse to accept cookies,

Updates

Chambers will occasionally update this Privacy Notice. When it makes significant changes, it will publish the updated Notice on Chambers' website at www.6pumpcourt.co.uk

PART FOUR – MEMBERS' OBLIGATIONS

This Part is applicable to barristers and pupils when acting as Data Controllers.

It is also relevant to Chambers' employees who should understand the information provided in relation to their own roles and responsibilities when acting for and on behalf of a barrister member.

In **Part Four** we set out:

The legal and regulatory requirements on barristers as Data Controllers.

Instructions to follow in order to meet the legal and regulatory requirements and the expectations of Chambers as set out in this Policy.

Introduction

As stated in **Part One** of this Policy Chambers makes available to all barristers a **Modern Desktop** system with **Managed Devices** designed to address the issues and matters discussed relating to Chambers' IT systems and ICT in this Policy.

Exceptionally Chambers may allow barristers to access and utilise Chambers' IT systems and services using **Self-Managed Devices** but only when the barrister has entered into a prior written agreement with Chambers to ensure that equivalent security provisions are in place. Such prior agreement must be in the form prescribed by Chambers in its **Bring Your Own Device (BYOD) Agreement**.

Nothing in this Part is intended to detract from or provide any other alternative to this approach and it should not be read as such.

Barristers must comply with this Policy and use it when formulating their own complementary Data Protection, Privacy and Information Security Policies as Data Controllers.

Legal and regulatory requirements on barristers

Core Duty 6 of the Bar Standards Board Handbook provides that it is a fundamental obligation of all regulated barristers to *"…keep the affairs of each client confidential"*. Further to the same, rC15.5 of the BSB Handbook states that all barristers: "*…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*".

It is the individual responsibility of each member of Chambers to preserve the confidentiality of their clients' affairs.

In the absence of specific instructions from instructing solicitors, this Policy and the guidance in this Part 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 UK GDPR applies. Such information is referred to in this Policy as "Confidential Material".

The ICO website provides detailed guidance on information security. Very substantial

monetary penalties may be imposed in the event of serious contravention of the UK GDPR. 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 ICO. In the event that a failure to keep information secure amounts to "serious misconduct", a barrister would be obliged to report this 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.

Barristers whose practice includes work for Government departments or agencies should also comply with the *Attorney General's Guidelines on Information Security and Government Work.*

The Receipt and Handling of Physical Materials

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

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

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, members should try to restrict the amount taken out to what is necessary.

Confidential Material should be moved securely. On public transport Confidential Material should not be left unattended. If travelling by private car, where practicable, Confidential Material should be kept out of sight and stored 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 out of the car. It should not be left in an unattended car overnight.

Physical Security of Electronic Devices

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

In particular members should not:

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

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 Mobile Devices

Particular risks to client confidentiality arise from the loss of Confidential Material held on

laptop computers, tablets, smartphones, 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 members 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 UK GDPR. Barristers should take as much care with this material as they would with their own valuables to prevent theft or loss.

Barristers should consider restricting the amount of Confidential Material stored on portable devices to the minimum necessary.

Electronic Security and Encryption

As set out in **Part One** of this Policy, barristers must use either a **Modern Desktop Managed Device** or a **Self-Managed Device the subject of a BYOD Agreement** between Chambers and the barrister member. By this approach it is the intention that the ICT and Information Security risks may be avoided so far as reasonably possible.

Barristers 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. This is particularly important when a barrister uses a Self-Managed device. If in doubt guidance should be sought from Chambers.

Care should be taken 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 members do not know and trust. Members should be especially vigilant concerning the risk of downloading malware by visiting websites which they 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 members should be wary of any link or attachment in an email which they were not expecting, even an email from an apparently known and trusted sender.

Access to computers, tablets, smartphones and other electronic devices containing Confidential Material should be protected by password. Members should take care to select a secure password. Passwords used to access computers or encrypted data should be sufficiently memorable that they can be avoided from being written down, but so that they are 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 passwords from time to time and in any event if it is disclosed to another person or discovered. Members 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.

Information stored electronically should be regularly backed up. 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.

Computers, tablets, smartphones and other electronic devices used at home to access Confidential Material should be protected from unauthorised and unrestricted access by third parties such as family members or house guests.

The ICO recommends that portable and mobile devices 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. Confidential Material stored on laptop computers and other portable devices (such as memory sticks, CD-ROMs, removable hard disk drives, tablets, smartphones and USB drives) should be encrypted in a reasonably secure manner, or as specified by the professional client. It is also appropriate to encrypt data stored on desktop computers. 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 unauthorised access to Confidential Material by shared users or other third parties

- 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

- Some device providers supply full device encryption which can be enabled by the user. Check with the supplier whether this applies to the relevant device. This encryption facility may not meet the requirements of a specific client, such as some Government Departments, in which case members should use the encryption standard required by their professional clients.

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.

Appropriate software should be used for encryption. The Bar Council does not endorse any individual software program or supplier. Not all encryption software meets the guidelines for barristers undertaking Government work.

Any device, code or password for the emergency recovery of encrypted material should be stored in a reasonably secure manner.

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 members' own, unless it is apparent that it is less secure. If it is apparent that the device or media is less secure, members should discuss this with their clients, including, where necessary, the lay client.

Communication

Email 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 email and if required by a client. In such cases members should agree with the client what encryption to use.

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

If members arrange for emails to be sent to their smartphone or tablet, they should ensure that the device is suitably password-protected and, if appropriate, encrypted.

Members should take care when using the 'auto complete' function that is offered by some email systems to ensure that they 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 data is not sent to the incorrect recipient.

Members of Chambers using a Chambers email address should take particular care to maintain the security of the email system, including by not opening attachments to suspicious emails, as viruses and malware may often spread upon infection by immediately emailing all of the account's contacts, which will necessarily include all of Chambers' email addresses. Chambers may suffer loss of service, data loss and significant reputational damage if this occurs.

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

The UK GDPR contains restrictions on the transfer of personal data to countries outside the UK and European Economic Area which do not provide an adequate level of security. For this reason, Chambers uses a reputable email service provider which is based, and provides email storage facilities, in the UK and European Economic Area. Accordingly, members should never have reason to use an email service other than Chambers' email system for the sending of Confidential Material.

Connecting to the internet via a wireless network presents a particular risk of interception of communication. Members should take particular care when connecting via public and unencrypted access points and should in any event refrain from making their computer detectable by others on the network. Members should, if practicable, use a virtual private network (VPN) to connect to unsecured wifi networks. If members use a wireless network system at home, they should ensure that it is reasonably secure.

CJSM Secure Email

Practitioners who are required to use CJSM secure email, in particular, criminal practitioners, must use the Chambers' email service where CJSM functionality has been incorporated.

Cloud Computing

As part of its **Modern Desktop** provision, Chambers provides barristers with a cloud based **OneDrive** system. All barristers are strongly encouraged to use it.

Barristers using alternative 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.

The UK GDPR contains restrictions on the transfer of personal data to countries outside the UK and 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 UK or European Economic Area should generally be used. If members use a service provider based elsewhere they 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. They 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.

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 use a cloud service provider whose software encrypts files before uploading.

Barristers who do not use the **OneDrive** system provided by Chambers should confirm the details of their chosen provision in their individual Data Protection, Privacy and Information Security Policy.

Chambers Matters

Reasonable steps should be taken to ensure the reliability of ICT and service providers that members contract with who might have access to Chambers' ICT systems. This would be likely to include checking identity and references. Even in relation to Chambers' staff, if in control of particularly sensitive documents, members may consider it necessary to prevent staff accessing them.

Barristers should undertake training on the importance of information security. Members should use training materials from the ICO and the Bar Council. Chambers also makes available suitable training for members to undertake.

Chambers has procedures in place for reporting any loss of electronic media or papers upon which or in which Confidential Material might be stored. When a loss or theft occurs, Chambers, the professional client and any appropriate third party such as the police should

be immediately informed.

Members should keep a log of devices upon which Confidential Material might be stored, including serial numbers, where available, and a record of encryption software installed. This will assist in the recovery of any lost or stolen items.

Data Minimisation and Disposal

It is a requirement of the UK GDPR that personal data (as defined in the UK GDPR) should not be retained for longer than is required. This length of time is decided by members depending upon their particular practice and may be up to **15 years** for case files.

Data retention, review and deletion schedules are part of Chambers' systems and in respect of barristers' own ICT systems. These schedules are implemented as an automatic review process by Chambers, in its capacity as a Data Processor in respect of data for which barristers are Data Controllers, as directed by barristers. Individual barristers will need to implement the schedules on their own ICT systems 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 UK GDPR.

Chambers has procedures in place for the secure disposal of Confidential Material and electronic media (e.g. the cross-cut shredding of papers and disks), and hard drives, and when disposing of Confidential Material via Chambers' systems (for example by disposing of papers in Chambers) members must always use the appropriate procedures.

Barristers who wish to dispose of any computer or electronic media upon which Confidential Material has been stored will ensure the material is effectively destroyed or wiped using a recognized 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.