RED LION CHAMBERS

18 RED LION COURT, LONDON

&

THORNWOOD HOUSE, CHELMSFORD

DATA SECURITY POLICY

INDEX

ANNEX

RED LION CHAMBERS

RED LION CHAMBERS DATA SECURITY POLICY

Introduction

In order to meet the requirements of the General Data Protection Regulation, we are obliged to have in place a framework designed to ensure the security of all personal data during collection, processing and disposal. We are committed to complying with relevant data protection legislation.

Scope of the Policy

This policy relates to the retention and storage of all personal data held in hard copy, i.e., on paper, or on physical devices, e.g., Laptops, PCs, Hard drives, USBs, CDs, DVDs, tablets and Smartphones, and the retention and use of electronic data.

This policy applies to all use of information and information technology on our premises, even if Chambers do not own the equipment, to all information technology provided by Chambers wherever it is used, including by employees working away from our premises, and to all external access to our information technology from wherever this is initiated, including by employees working away from our premises.
Further information and guidance is available from our DPL or Instanton.it [https://www.instantonit.com]

This policy applies to all *members*, probationary tenants, employees, agency staff, contractors, mini pupils & pupils and other third parties who on occasion are granted authorised access to Chambers' data and systems. All members (as Data Controllers) are responsible for their own data security. However, the following procedures will be applicable to members who are processing Chambers' data in their capacity as a member of chambers, a committee member or other such determined reason which may arise.

Keeping Personal Information Secure

All personal data, whether in hard copy or stored on a USB, CD, DVD, or other physical device, must be kept in a secure environment with controlled access. The level of security applied should be agreed after a basic risk assessment has been carried out as provided for below. Appropriate secure environments include:

- locked metal cabinets with access to keys limited to authorised personnel only;
- locked drawers in a desk (or other storage area) with access to keys limited to authorised personnel only; and
- locked rooms accessed by key and/or coded door lock where access to keys and/or codes is limited to authorised personnel only.
- Privacy filters should be installed on all laptops as a matter of course. They can be easily obtained from Amazon. These reduce risk of inadvertent disclosure of data when travelling, at Court or indeed in Court. There has been a warning from the Circuit that the displacement of jurors around the Court room due to social distancing means on occasion jurors have been able to see what is on Counsel's laptops. For obvious reasons this is ill-advised.

All staff must receive appropriate induction on data security in general and specific data security requirements in their area of business.

Where access to personal data is required on a frequent basis, and therefore maintaining locked drawers or cabinets at all times is impractical, steps must be taken to ensure authorised personnel are in attendance at all times when the data is in an unlocked environment.

Files containing personal data must never be left unattended while removed from their normal locked storage area. Staff must therefore adopt a clear desk policy, in relation to files and documents containing personal information, at all times when they are out of their offices or away from their work area.

Access to Personal Data

Mark Bennett the Practice Director or Nick Parkinson the Deputy Practice Director (for present purposes 'the Manager or Managers') must designate the individual members of staff who, by nature of the post, have been identified as requiring legitimate access to personal data in the course of their duties.

In addition, the designated purposes for which access to personal data will be permitted must also be defined. For some business areas, this will be clear from the function of the business area, e.g., Human Resources. However, in other cases this will require to be specifically defined.

From time to time all staff will have access to personal data about other members of staff or members and confidentiality must be observed by all staff at all times. When temporary staff are employed in posts which involve access to and processing of personal data, confidentiality agreements should be included within the Terms and Conditions of Employment.

Where a file containing personal data is removed in response to a legitimate request by another authorised member of staff, this must be subject to a strict signing out and return procedure, which is the responsibility of the person holding the file.

The Manager of the relevant area will be expected to designate a member of staff with responsibility for overseeing arrangements for the removal and return of records.

The occasions when personal information is photocopied should be kept to a minimum. Where this is necessary, the provider of the information is responsible for ensuring all copies are returned once the task in question has been completed and subsequently disposed of in accordance with our Retention and Disposal Policy.

Where employees are required to take manual personal data home with them, appropriate security precautions must be taken to guard against theft, loss or inappropriate access. This will include securing data in a locked briefcase, never leaving data unattended in a public place and ensuring that all reasonable precautions are taken to secure data at home and whilst in transit. When working from home staff are required to use secure remote access to electronic records containing personal data and should not copy such records to a home PC. See Appendix 1 and Chambers Remote Working Policy for more detailed guidance.

Staff should ensure that visitors for whom they are responsible are signed in and out upon arrival in the building and are accompanied in areas normally restricted to staff.

Risk Assessment

A data protection/security risk assessment will be carried out as appropriate by business area managers or by an individual designated by them.

The purpose of the assessment is to establish the potential risks for unauthorised access to personal data and to define appropriate actions to eliminate, or at least mitigate, the risk of unauthorised access.

Managers will be expected to consult the Data Protection Lead on steps planned to address any potential risks identified.

Third Parties

Arrangements must be in place to ensure the security of all personal data which may be transferred to, or processed by, a third party.

In advance of any external transfer of personal data, staff are required to consider whether such a transfer is authorised under any relevant data sharing agreement or is otherwise required by or permitted under the General Data Protection Regulation. The purpose, fairness and transparency of any transfer must always be considered, and staff must ensure that they have consulted the Data Protection Officer/Lead prior to any such external data sharing.

Where external data sharing has been considered necessary or is permitted, the appropriate security precautions should be taken to minimise the risks of loss of data and/or accidental third-party disclosure.

All communications should be marked strictly private and confidential and addressed to a named individual.

Physical devices containing personal data, e.g., USBs, CDs, DVDs, must always be encrypted before being removed from our premises.

The most appropriate secure method of sending the information must be considered, e.g., hand delivery, registered or recorded delivery, courier, encrypted or secure electronic transfers.

Disposal of Personal Data

Personal data will be retained only for the designated periods in our Retention and Disposal Policy. The Data Protection Leads will provide further advice and guidance on request.

All personal data must be disposed of securely and safely in accordance with the Retention and Disposal Policy.

Electronic Devices

The electronic storage of personal data requires certain minimum levels of security.

a. All personal computers/devices used for work must be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans, and protected by a firewall appropriate for the computer used.
b. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
c. Access to all computers must be password protected.
d. Particular care must be taken to avoid potential infection by malware, e.g., by downloading software other than from trusted sources.
e. Work-in-progress should be regularly backed up, and back-up media should be locked away securely.
f. Computers used for working on personal data at home should be protected from unauthorised and unrestricted access by third parties, including family members. Where practicable, the ideal is a computer used only for work.
g. The use of removable storage media (such as memory sticks, CD-ROMs, removable hard disk drives and PDAs) is prohibited without the express authorisation of the Data Protection Leads and only in particular circumstances
h. Laptop computers must be encrypted to such standards as may be approved by the Instanton.it

Chambers is looking via Instanton.it to introduce a system whereby a device will only be able to log into the Chambers network if it is encrypted and has all its software up to date.

Chambers maintains a log of all computers and devices used for storing or working on personal data. The log is maintained by the Joe Barrett (Administration and Financial Management) and records type, model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine. Only use devices that are on this log.

Security Incidents

All incidents where the security of personal data or IT systems has been compromised or where there have been any suspected security weaknesses or threats must be reported immediately to the Data Protection Leads

The Chambers Information Security Committee in conjunction with Data Protection Leads will decide in the particular circumstances of the breach whether it is serious enough to inform the Information Commissioner's Office.

Any breach of security policies and procedures by a member of staff will be dealt with through the relevant formal disciplinary processes.

Business Continuity and Disaster Recovery

All IT systems have been subject to a formal risk assessment exercise to determine their level of criticality to the organisation and to determine where and at what level business continuity planning is needed. The business has also developed guidance on its vital manual records and the appropriate business continuity measures to be adopted for all electronic and manual data. Designated control measures ensure that manual personal data is kept in an appropriately secure environment where risk of loss or damage is minimised.

Appropriate arrangements must be made for manual records which are classed as 'vital records', including fire-proof storage, off-site storage and backing up in electronic form e.g., by scanning. However, as electronic copies of such records may not provide the same evidential weight as the original document, the Manager with responsibility for such records must consider which arrangements are appropriate and seek advice as necessary from the Data Protection Leads.

Chambers must ensure that the vital records register held within their Business Continuity Plan is regularly reviewed and updated as required.

APPENDIX 1

Good Practice Guidelines

General

1. Set an auto lock time on all workstations used so that they lock automatically after no more than 5 minutes of inactivity.
2. Always log off or lock a workstation before leaving it. This is to ensure that no one else can access your information or has the opportunity to use your workstation without identifying themselves, e.g., to send an abusive email in your name.
3. When confidential work is being carried out ensure no one else can read the screen.
4. Protect equipment from physical theft. This is vitally important for portable equipment.

5. Ensure that all data is backed up regularly and copies kept in a separate secure location. Liaise with Joe Barrett or Instanton.it if you require assistance.
6. Respect the legal protections for information and software provided under copyright and licenses. Never copy electronic information or computer programmes unless specifically authorised in writing. Never run or install software without a valid licence.
7. All PCs should be patched with the latest security critical and up to date patches.
8. All data storage devices including laptops, USB sticks, CD's, DVD's that are brought into the business must be checked for viruses on every occasion before use.
9. All workstations connected to our network, whether owned by us or not, shall be continually running approved virus-scanning software with a current virus database.
10. Never introduce malicious programs into our network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) by any means.

Email and Internet Use

1. Always check the address line before sending a message and check it is being sent to the correct person.
2. Never represent yourself as another person or persons.
3. Delete electronic mail messages when they are no longer required.
4. Do not make comments or express views that could be regarded by others as offensive or libellous.
5. Personal private emails must be saved in a separate folder from work related emails. Clearly mark all emails that are of a personal nature as "personal".
6. Personal/private postings to blogs, newsgroups or similar which mention our business must contain a disclaimer stating that the opinions expressed are strictly personal and not necessarily those of our business.
7. Do not open e-mail attachments received from unknown senders as these may contain viruses, e-mail bombs, Trojan horse code or some other form of Malware.
8. Do not forward electronic mail messages that have been sent to you containing personal data (as defined by the General Data Protection Regulation) to other individuals or groups without the permission of the originator.
9. Do not participate in chain or pyramid messages or similar schemes.
10. Do not unnecessarily send excessively large electronic mail messages or attachments.
11. Report any unusual or suspect email messages or network activity to Instanton.it.

Social Media

Where employees use Chambers social media accounts or use personal social media accounts in a work-related capacity they must not:

1. Post statements or share links to content that may be considered defamatory, inappropriate or result in potential litigation proceedings. Such content to include but not limited to material which could reasonably be considered as offensive on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law or comments which may be considered as offensive or harassment.
2. Use social media for any illegal or criminal activities.
3. Broadcast unsolicited views on social, political, religious or other non-Chambers related matters.
4. Send or post messages or share material that could damage Chambers and its members' image or reputation.

5. Make comments about work colleagues, Members of Chambers, clients or competitors,
6. Post, upload, forward or link to spam, junk email or chain emails and messages.
7. Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
8. Share links to illegal copies of music, films, games or other software.
9. Share or link to data in any way that could breach the company's data protection policy.

Passwords

1. All workstations must be protected with a password. This function is carried out by the Managers.
2. Authorised users are responsible for the security of their passwords and user accounts. Passwords must be kept secure and never shared with anyone else.
3. Passwords must be [at least 7 characters long and include alpha, numeric and at least one other character]. Their structure must make them hard to guess. Guidance on creating passwords is available from the Managers or from the National Cyber Security Centre: [https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0]
4. Passwords should never be displayed on screens.
5. If at any time you think someone may have discovered your password, you must immediately change it or request that it is changed.
6. At times, normally when the user has forgotten their password, it will be necessary for passwords to be changed by Managers In these cases, proof of identity will be required as for account/password creation.
7. Passwords should never be "remembered" on the computer but entered by the user on all occasions.

Securing Personal Data during Off-site Usage

Transferring papers to Court

1. Papers should stay with any member of staff or pupil you until you have handed the papers over to the barrister who is in court.
2. Where possible use locked cases or if that is not feasible try to cover the name of the case, by using a bag or similar to cover the boxes.
3. When collecting papers from the court, you should ensure these are kept under your control until they are returned to the barrister's room.

Paper Records

- All files or papers leaving chambers are to be stored in an appropriately secured bag, e.g., a briefcase, which has a lock.
- All items used to carry papers should have a security message clearly displayed such as:

'This is the property of Red Lion Chambers. If found please contact us at 0207 520 6000 urgently or return to Red Lion Chambers, 18 Red Lion Court, London, EC4A 3EB. This is a secure document holder that may contain confidential information. Any interference with the material or attempt to access it is strictly prohibited. '

- Files or papers must never be left freely available in any common area where it may be read by other individuals, e.g., in court, on a train or bus, in coffee shops, at home. **This may require a real change in behaviour in terms of material left in Court rooms. We have real concerns that present practice of leaving papers**

unattended in Court rooms is problematic. Even if Court staff are present, they are not acting as keepers for members papers.

- Files or papers must not be left in a position where another person entering the room or looking through a window might read them inadvertently.
- Files or papers must never be read or worked on in a public area, including working on phones or laptops, where members of the public can read them.
- An employee may work on files or papers at home provided that the material is put away in a locked non-portable container when not in use. There must be appropriate physical security measures in any place files are stored, for example, the use of burglar alarms, a lock on the room the files are in, etc.
- All files and papers must be moved securely. They should not be left unattended on public transport. If travelling by private car, where practicable, keep them out of sight and stored as inconspicuously as possible. Files and papers should not be left unattended in a car except where the risk is less of a risk than taking them with you. They should never be left in a car overnight.
- Staff should not dispose of hard copy papers that contain any personal data outside the office. This includes handwritten notes, post-its etc. All hard copy paper disposals are to take place in the office to meet shredding standards.
- Members disposing of papers outside Chambers must either shred the material themselves or when dealing with larger volumes of material use an external shredding service and obtain a certificate to demonstrate secure destruction.

Electronic Devices

1. The electronic storage of personal data requires certain minimum levels of security.
   a. All personal computers/devices used for work must be recorded as used for work by Chambers Device log or the members own personal logs and must be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans, and protected by a firewall appropriate for the computer used.
   b. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
   c. Access to all computers must be password protected using sensible not easily guessed passwords.
   d. Particular care must be taken to avoid potential infection by malware, e.g., by downloading software other than from trusted sources.
   e. Work-in-progress should be regularly backed up, and back-up media should be locked away securely.
   f. Computers used for working on personal data at home should be protected from unauthorised and unrestricted access by third parties, including family members. Where practicable, the ideal is a computer used only for work.
   g. Storage mediums and devices such as USBs, external hard drives, flash cards and any other portable drives carry considerable risks in transporting, storing or transferring confidential business information. Therefore, the use of removable storage media is prohibited without the express authorisation of the Data Protection Lead, and encryption should always be used.
   h. Laptop computers must be encrypted to FIPS 140-2 or CCTM (CESG Claims Tested Mark) standards, or to such other standards as may be specifically approved by Instanton.it. Whole disc rather than folder encryption is required. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60968/cross-gov-actions.pdf]

i. The organisation maintains a log of all Chambers computers and devices used for storing or working on personal data. The log is maintained by Joe Barrett and records type, model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine. Only use devices that are on this log.

2. To ensure safe remote working you should ensure that:

a. You have suitable encryption software installed for the storage and transportation of business information.

b. Business information should not be stored or transported using a mobile device unless there is a clear business need to do so and should be retained only temporarily to fulfil that need. The information should then be adequately deleted and unrecoverable from that device.

c. If the device is to be used to handle data provided by a third party, it is the device owner's responsibility to ensure any security or data handling requirements by that organisation are met.

d. Users must ensure they mitigate the risks associated with the environment in which they may be working. Advice and guidance should be sought from the Data Protection Leads on environments, out-off-office or international locations where you may be unsure of the risks you may be facing. It is hard to conceive of staff needing to access Chambers data from international locations.

e. Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Users therefore must ensure that no confidential information should be synchronised to or stored on cloud-based storage that has not been specifically agreed by the Managers or Instanton.it on behalf of the business.

f. Should the loss, theft or misplacing of any such device occur, Chambers Information Security Committee (isc@18rlc.co.uk) should be immediately informed with as much detail as possible regarding the device, the data it held and whether the loss had been reported to any relevant authorities.

g. If you access e-mails from your mobile telephone or Smartphone, you must ensure that the device is suitably password-protected and encrypted. In addition, all employees will operate an 'inbox-zero' policy so that the number of emails stored on any device is at a minimum.

3. Computers or devices must not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.

4. Extreme care should be taken to ensure that laptops, removable devices, and removable storage media containing personal data are not lost or stolen. In particular, such laptops and other removable devices should never be left unattended in public places or left in a car overnight.