ST JOHN STREET CHAMBERS

Template 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. USBs, CDs, DVDs, tablets and Smartphones, and the retention and use of electronic data. It should be read in conjunction with the Computers, Telecommunications, Internet and Social Media Policy.

This policy applies to all use of information and information technology on our premises, even if we do not own the equipment, to all information technology provided by the business 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 the chambers privacy officer, Emma Bowie.

This policy applies to all employees, including temporary and casual employees, and agency staff.

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:

- Chambers-provided 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.

For all platforms processing personal data, including LEX, Microsoft and other chamebrs systems, all security settings must be set to their highest possible setting by default, and only lowered for operational reasons where required. Multi-Factor Authentication **must** be enabled across all systems which process client file data, including staff personal mobiles where chambers data is accessed.

All staff must receive appropriate induction on data security in general and specific data security requirements in their area of business no less than annually.

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

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. Access will be administered on a Least Privilege basis by default for client data systems. Staff will not have access to client data unless this is clearly required in line with 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 may have access to personal data about other members of staff or clients 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.

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 for more detailed guidance.

Members and staff must ensure that visitors for whom they are responsible are signed in and out at reception and are accompanied in areas normally restricted to staff.

Risk Assessment

A data protection/security risk assessment will be carried out as and when appropriate by the Data Officer or by an individual designated by them. Such assessments should be carried out when chambers migrates IT provider or introduces a new system or process which impacts upon the processing of client personal data.

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.

Relevant team leaders will be expected to consult the Data Officer 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 UK GDPR. The purpose, fairness and transparency of any transfer must always be considered and staff must ensure that they have consulted the Data Officer 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. Sensitive attachments should never be sent without first encrypting or password protecting them.

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 to a minimum of AES-256 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. For electronic transfers, encrypted file-sharing solutions should always be used, such as Sharepoint, Tresorit, Dropbox, WeTransfer.

Disposal of Personal Data

Personal data will be retained only for the designated periods in our Retention and Disposal Policy. The Data Officer, **Emma Bowie,** will provide further advice and guidance on request. The Data Officer can be contacted at **ebowie@18sjs.com.**

All personal data must be disposed of securely and safely in accordance with the chambers 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. Updates may only be delayed a set number of times, after which you **must** allow a full restart for updates to take effect.
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. **Passwords must for 18SJS systems must be a minimum of 8 characters and include at least 1 number and one special character.**
d) Particular care must be taken to avoid potential infection by malware, e.g. by downloading software other than from trusted sources. Any introduction of malware into the 18SJS environment as a result of accessing unsafe websites will be investig
e) 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.
f) The use of removable storage media (such as memory sticks, removable hard disk drives and PDAs) is prohibited without the express authorisation of the Data Officer, and only in particular circumstances as specified by the Data Officer.
g) Laptop computers must be encrypted to such standards as may be approved by the IT manager, typically AES-256.

18SJS maintains a log of all computers and devices used for storing or working on personal data. The log is maintained by external IT support, Instant On IT, 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.

ST JOHN STREET CHAMBERS

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 Officer using the internal Breach Reporting Form.

The Data Officer will THEN 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 Officer.

For further information, please see our **Business Continuity Policy.**

ST JOHN STREET
CHAMBERS

Appendix 1

Good Practice Guidelines

General

1. 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.
2. When confidential work is being carried out, ensure no one else can read the screen.
3. Protect equipment from physical theft. This is vitally important for portable equipment. **Never** leave work devices unattended outside of chambers or your home.
4. Ensure that all data is backed up regularly and copies kept in a separate secure location. Liaise with the IT Department if you require assistance.
5. 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.
6. Never run or install software without prior approval from chambers' IT provider.
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 in to 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. Take care when using autocomplete as this can lead to inadvertent breaches.
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 unnecessarily send excessively large electronic mail messages or attachments.
10. Report any unusual or suspect email messages or network activity to the IT Department.

Passwords

1. All workstations must be protected with a password. This function is managed by Instant On IT, and the Data Officer reserves the right to vary password complexity rules as required to protect the business.
2. Avoid using the same password for multiple accounts and devices. Doing so will help to minimise the impact of a single compromised login.
3. Authorised users are responsible for the security of their passwords and user accounts. Passwords must be kept secure and never shared with anyone else.
4. Passwords must be [at least 8 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 Instant On IT.
5. Passwords should never be displayed on screens.
6. If at any time you think someone may have discovered your password you must immediately change it or request that it is changed.
7. At times, normally when the user has forgotten their password, it will be necessary for passwords to be changed by [the IT Department]. In these cases, proof of identity will be required as for account/password creation.
8. Passwords should never be “remembered” on the computer but entered by the user on all occasions.

Securing Personal Data during Off-site Usage

Paper Records

1. All files or papers leaving the office are to be stored in an appropriately secured bag, e.g. a briefcase, which has a lock.
2. All items used to carry papers should have a security message clearly displayed such as;
    a. ***This is the property of [ ]. If found please contact us at 0161 278 1800 urgently or return to 18 St John Street Chambers, 18 St John Street, Manchester, M3 4EA. This is a secure document holder that may contain confidential information. Any interference with the material or attempt to access it is strictly prohibited and may constitute a criminal offence.***

3. Files or papers must never be left freely available in any common area where it may be read by other individuals, e.g, on a train or bus, in coffee shops, at home.
4. 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.
5. Files or papers should never be read or worked on in a public area, including working on phones or laptops, where members of the public can read them.
6. 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.
7. 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.
8. Do 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.
9. All hardcopy documents must be safely locked away in secure cabinets at the end of each working day and outside of office hours.

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 registered with Instant On IT 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.
    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 Officer/Lead, and encryption should always be used.

h. Laptop computers must be encrypted to AES-128 or 256 standards, or to such other standards as may be approved by Instant On IT. Whole disc rather than folder encryption is required.
i. All data which constitutes client file data must be sent only in an encrypted form using a dedicated encryption software or platform (such as Tresorit, WeTransfer or Egress). Further training on encryption best practice will be delivered at regular intervals.
j. The organisation maintains a log of all computers and devices used for storing or working on personal data. The log is maintained by the [IT department] 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 mobile working you should ensure that:
    a. You have suitable encryption software installed for the storage, sending 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 Instant On IT on environments, out-off-office or international locations where you may be unsure of the risks you may be facing.
    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 agreed contractually by the Data Officer on behalf of the business.
    f. Should the loss, theft or misplacing of any such device occur, the Data Officer 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.

If you have any questions regarding this policy or your duties under the policy, please contact the Data Officer at **ebowie@18sjs.com**

ST JOHN STREET
CHAMBERS

Date of last Review:	Reviewed by:	Reviewer comments:	Date of next Review: