DATA SECURITY POLICY FOR SELBORNE CHAMBERS LIMITED

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.

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 Sarah Walker.

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.

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

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.
From time to time all staff will have access to personal data about other members of staff or customers and confidentiality must be observed by all staff at all times.

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.
Staff should ensure that visitors for whom they are responsible are accompanied in areas normally restricted to staff or members.

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 Officer/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.

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

DISPOSAL OF PERSONAL DATA

Personal data will be retained only for the designated periods in our Retention and Disposal Policy.

The Data Protection Officer/Lead 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) Laptop computers must be encrypted.

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 Officer.

The Data Protection Officer/Lead 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.

Review Data	Reviewed
12 June 2019	IJC

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.

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. Never run or install software without a valid licence.

6. All PCs should be patched with the latest security critical and up to date patches.

7. 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.

8. 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.

9. 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 the IT Department.

Passwords

1. All workstations must be protected with a password. This function is carried out by the IT Department.

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 should never be displayed on screens.

4. If at any time you think someone may have discovered your password, you must immediately change it or request that it is changed.

5. At times, normally when the user has forgotten their password, it will be necessary for passwords to be changed by the IT Department.

6. 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

- All files or papers leaving the office are to be stored appropriately.

- Files or papers must never be left freely available in any common area where it may be read by other individuals, e.g. in a client's office, on a train or bus, in coffee shops, at home.

- 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.

- 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.

- 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.

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 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. Whole disc rather than folder encryption is required.

2) To ensure safe mobile 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 IT Department 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 IT Department on behalf of the business.

f) Should the loss, theft or misplacing of any such device occur the IT Department 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 when working in 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.