City Lord Ltd
DATA PROTECTION, INFORMATION MANAGEMENT AND SECURITY POLICY

Data Protection Policy

We are fully committed to compliance with the requirements of the General Data Protection Regulations which comes into force on 25 May 2018.

It is the responsibility of Miss Sidrah Butt as the DPO to ensure that:

- the Company is registered with the Information Commissioner's Office (ICO) for all necessary activities under the Regulation;
- there is a process of continual review to determine whether any changes in the company's registration are required as a result of changes in the nature of the business;
- the details of the Company as registered are kept up to date;
- the notification to the ICO is renewed annually;
- the Company maintains and updates the public Data Protection Register which will be reviewed regularly and at least on an annual basis;
- report any data breaches, including cyber-attacks and accidental leaks within 72 hours to the ICO;
- where individuals request a copy of all personal data held such data will be supplied promptly and no later than 30 days without charge; and
- the Company maintains this policy.

We are aware of and adhere to the six data protection principles which underline the Regulations, namely that all data which is covered by the Regulations (which includes not only computer data, but also personal data held within a filing system) is:

- processed lawfully, fairly and transparently;
- collected only for specific legitimate purposes;
- adequate, relevant and limited to what is necessary;
- must be accurate and kept up to date;
- stored only as long as is necessary; and
- ensure appropriate security, integrity and confidentiality.

All members of staff are provided with training on Data Protection compliance on induction and as necessary from time to time. Additional training on any changes to this policy and refresher training will be provided annually.

Any member of our staff with an enquiry about the handling and processing of personal data should approach who is responsible for data protection in our Company.

Each staff member is responsible for ensuring that no breaches of this policy result from their actions. Failure to comply with this policy by any member of staff may invoke our Disciplinary Procedure and may result in disciplinary proceedings.

Each staff member is responsible for reporting any breach, or suspected breach of this policy to our DPO, Miss Sidrah Butt who will conduct an incident management plan in accordance with our Information Management and Security Policy.

Miss Sidrah Butt will undertake an annual review of this policy to verify it is in effective operation.

Subject access requests

Any individual whose data is held by the Company may make what is called a 'subject access request', i.e. a request to see what data is actually held about them. All such requests should be addressed in writing to Miss Sidrah Butt and she will arrange for the Company to comply promptly with the request and no later than 30 days.

Information Management and Security Policy

The information we hold is both extremely sensitive and valuable. If this information is mismanaged there could be serious repercussions for our clients, other individuals as well as for the Company.

Our policy is to protect the information we hold from all threats, whether internal, external, deliberate or accidental.

It is our policy to ensure that:

- information is protected against unauthorised access;
- information is kept confidential;
- the integrity of information we hold is maintained;
- regulatory and legislative requirements are met;
- all breaches of information security, actual or suspected are reported and investigated; and
- business and individual requirements for the availability of information and information systems are met.

We maintain the security and confidentiality of the information we hold as well as our information systems and applications by:

- ensuring that all staff are aware of and fully comply with all relevant UK and European legislation including, but not limited to,

    - the General Data Protection Regulations;
    - the Data Protection (Processing of Sensitive Personal Data) Order 2000;
    - The Copyright, Designs and Patents Act 1988;
    - The Computer Misuse Act 1990;
    - Regulation of Investigatory Powers Act 2000;
    - Freedom of Information Act 2000

- having a consistent approach to security by ensuring that all staff are aware of the information security policies and procedures applicable in their work area and fully understand their own responsibilities;

- creating and maintaining within our Company a level of awareness of the need for information security and data management as an integral part of our day to day business;

- having in place up to date contingency and recovery plans;

- having in place measures to ensure data is secured against loss and unauthorised access;

- protecting the information assets under our control.

The information the Company hold falls within three categories:

- Information in relation to the Company's business,
- Information in relation to Employee's HR records and Pay roll; and
- Information relating to Company's clients.

Information Assets

An assessment of all assets and all information held by us is made annually by our DPO, Miss Sidrah Butt to ensure that appropriate procedures are in place to mitigate the risks.

The register below lists the key information assets we have identified for our Company. Additionally, the register considers the risks to these assets, their likelihood and impact and how we ensure the protection and security of the assets.

Our Assets	Risk	Likelihood	Impact	Method of protection/security
Business Plan	Low	Low	High	Access only with consent of our Directors. Backed up on external hard-drive.

Financial Information	Medium	Medium	High	All information kept by our COFA. Access only with his consent. Backed up on external hard-drive.
Accounts Information	Medium	Medium	High	All information kept by our COFA,. Access only with his consent. Copies of accounts information held by external accountants. Backed up on external hard-drive.
Recruitment & Employment records including equality & diversity monitoring information about staff	Medium	Medium	High	All information kept in by the Practice Manager and DPO with access restricted to the Practice Manager and Directors.
Complaints Information	Low	Low	High	Complaints information kept in DPO's office. Access restricted to the Practice Manager and Directors.
Money Laundering disclosures	Low	Low	High	All money laundering data is kept by our MLRO. Access restricted to the Director.
Case management system	Low	Low	High	This system is backed up onto external hard-drives.
Original documentation held on behalf of clients	Medium	Medium	High	These documents are kept in the relevant file and stored securely in locked cabinets.
Computers and IT	Medium	Medium	High	Computers are password protected and passwords are changed regularly. The use of memory sticks and other removable media is only used when there is a business case and all such data will be

				encrypted. New IT systems and upgrades are authorised by our DPO following an appropriate risk or impact assessment. The authorisation process takes into account our security requirements.

Register of all software

The table below outlines all software used by the Company.

Name of Software	Version	Installation date
Microsoft Office	2010	

Measures to ensure the adequate physical security of our premises that are used to store, process or access our information assets are considered in our Business Continuity Plan.

Specific measures which we have put in place to ensure the protection and security of all of our information assets include:

- ensuring that all equipment is physically protected from threats and environmental hazards;
- ensuring that only authorised persons who have a justified business need are given access to any restricted area containing information systems or stored data;
- ensuring access controls are maintained at appropriate levels; and
- information will only be held as long as is required and disposed of in accordance with our File Storage and Destruction Policy.

Access Controls

Individual user accounts are managed by Miss Sidrah Butt. She has responsibility for authorising new user accounts and for maintaining necessary access levels or other controls over existing accounts. Access rights will not be provided/amended without the prior authentication and authorisation by Miss Sidrah Butt.

Requests for new accounts or requests by existing users for amendments or adjustments to access rights must be made to Miss Sidrah Butt. She will conduct checks and assess any risks associated with the request. Only when she is satisfied that all risks have been identified and any necessary control measures implemented will the account be created/modified.

Any limits on access will be confirmed to the user prior to authorisation. Staff members' user rights generally cease upon termination of their employment contract, unless otherwise expressly agreed in writing by Miss Sidrah Butt. Other controls on user rights will be set by and monitored by Miss Sidrah Butt.

User accounts shall only be used by the person (or persons) it was issued to. Each user is responsible for the appropriate use of their accounts.

Miss Sidrah Butt will monitor the use of user accounts in accordance with this policy.

Access controls to our computerised bank accounts are designated by our Directors in accordance with our financial procedures.

Computers *& IT*

All network devices, whether they are computers, printers, tablets or other pieces of equipment that can connect to and communicate over the internet, are configured securely in accordance with current ICO guidelines. In particular, Miss Sidrah Butt will conduct a monthly review of our network and devices to determine if further steps are required to ensure the security of our systems.

Steps that we currently take, and which are reviewed include:

- updating passwords on our router;
- ensuring that all of our computers are password protected and that passwords are changed on a regular basis. The setting of new passwords and the maintaining of records are overseen by our Directors. Records of all passwords are maintained confidentially by our Directors;
- using encryption software;
- ensuring anti-virus and anti-spyware is installed on all of our computers, laptops, servers and other electronic media and kept up to date; and

- Computers and other devices are locked whenever they are not in use.

Our network is protected by the use of software firewalls which are built into our computer operating system. We also have a hardware firewall (a router) in operation.

All electronic data is securely backed up at the end of each working day. Records are maintained by Miss Sidrah Butt of all backup information including any failures or other issues. Backup media is encrypted and, where retained on-site prior to being sent for remote storage is stored securely in a locked safe and at a sufficient distance away from the original data.

The disposal of any computers or electronic media is overseen by Miss Sidrah Butt to ensure that appropriate destruction methods are used.

Removable Media

We appreciate that there are large risks associated with the use of removable media (i.e. any medium which can be removed from the workstation including DVDs and USB storage devices). The use of removable media devices is only approved if a valid business case for its use is developed. Requests for access to, and use of, removable media devices must be made in advance to Miss Sidrah Butt.

Should access to, and use of, removable media devices be approved the following must be adhered to at all times:

- the only equipment and media used to connect to the Company's equipment is that which has been purchased by the Company and approved by Miss Sidrah Butt;

- in all cases where the data/information to be held on the removable media device or laptop could be used to cause any individual damage or distress, in particular where it contains financial or medical information, the data/information must be encrypted before it will be permitted to leave our premises;

- removable media should not be the only place where data is held. Copies of any data stored on removable media must also remain on the source system or computer;

- in order to minimise physical risk, loss, theft or electrical corruption, all removable storage media is stored in an appropriately secure and safe environment;

- all data copied to any removable media is deleted as soon as possible from that media; and

- each member of staff is responsible for the appropriate use and security of data in accordance with this policy and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

Third Parties

Third parties including Landlords, may not receive data or IT equipment without explicit agreement from Miss Sidrah Butt. Should third parties be allowed access to such information or systems then the Company ensures that this policy is applied in full to their use, storage and transfer of the data.

Clear Desks Policy

A clear desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an employee's workspace and locked away when the files are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilise when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

The purpose for this policy is to establish the minimum requirements for maintaining a "clear desk" – where sensitive/critical information about our employees, our client, and our intellectual property is secure in locked areas and out of site. A Clear Desk policy is a part of our standard basic privacy controls.

This policy applies to all employees and associates. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

As part of the Clear Desk Policy, all staff must ensure the following:

- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Whenever desks are unoccupied for any extended period and at the end of each working day, all casefiles and other confidential information are removed from desks and securely locked away.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

- Whiteboards containing Restricted and/or Sensitive information should be erased.

- Lock away portable computing devices such as laptops and tablets.

- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Transfer of data

Confidential or other data is not removed from our offices unless a valid business case for its use is developed. Requests for permission to remove data or other information are made in advance to Miss Sidrah Butt. Where information is permitted to be removed, all reasonable steps are taken to ensure that the integrity and the confidentiality of the information are maintained including:

- keeping files and information is a secure and locked environment;

- transporting files and information securely; and

- not leaving files or information unattended in places where they are at risk (such as in cars, conference rooms or other public places).

In all cases, the terms of our Data Protection and Confidentiality Policy must be adhered to.

We conduct verification checks on all postal, fax and email addresses before any information is sent to them. All sensitive or confidential information is encrypted before being sent by electronic means or sent by tracked or recorded delivery.

Software

All software must be authorised by Miss Sidrah Butt who is responsible for planning and managing all information security risks and for overseeing its installation. In order to ensure we preserve the security and integrity of our systems and data, she is responsible for:

- maintaining our software register which records details of all software used by our Company;

- conducting a quarterly review of our software register;

- maintaining a plan for monitoring and updating all software used by our Company to ensure that all software is kept up to date, continues to be appropriate for our Company and works efficiently. As part of the implementation of this plan, reviews are conducted of all systems in order that any faulty or malicious software may be detected, removed and, if necessary, replaced by an alternative product; and

- reporting all changes to the plan are communicated to relevant staff members.

It is the responsibility of all staff to ensure they use software legally in accordance with relevant licensing and copyright agreements. Copying software for use outside of these agreements is illegal and may result in criminal charges.

Compliance & Incidence Management

All staff must comply with information management and security procedures including the maintenance of data confidentiality and data integrity. They are also responsible for the operational security of any information systems they use including our case management system.

All staff members are provided with training on this policy and security procedures during their induction. Additional training on any changes to this policy and any necessary refresher training is provided annually.

Each staff member is responsible for ensuring that no breaches of this policy result from their actions. Failure to comply with this policy by any member of staff may invoke our Disciplinary Procedure and may result in disciplinary proceedings.

Any actual or suspected breaches (or the risk of such a breach) in information or data security shall immediately be reported to our DPO, Miss Sidrah Butt. She will, in respect of any breach, consider an appropriate incident management plan to include:

- immediately invoking any necessary procedures to contain the breach and limit the adverse consequences;

- assessing any risks associated with the breach to determine the gravity of the breach and whether it is a serious breach of any appropriate legislation or regulations;

- determining what needs to be done when the breach is contained;

- notification to all relevant individuals and bodies such as the Information Commissioner's Office within 72 hours, other third parties such as the police or banks; and

- evaluating the causes of the breach and ensuring that any unsatisfactory procedures are corrected.

Miss Sidrah Butt is responsible for implementing our Information Management and Security Policy and for monitoring compliance. He undertakes an annual review of the policy to verify it is in effective operation.

Acceptable Use of the Company's IT Facilities Policy

All of the Company's IT facilities and information resources remain the property of the Company and not of any individual staff member.

Staff members may use the Company's computers, networks or domains for personal use but must do so in accordance with this policy and our E-mail policy. Staff members should not use the Company's computers, networks or domains to create or store personal or non-work related documents.

No member of staff must attempt to gain unauthorised access to information (including other people's files or restricted information). The Computer Misuse Act 1990 makes it a criminal office to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents.

Internet Access

All staff members have a duty to use the Internet responsibly. Acceptable uses of the internet are as follows:

- research;

Any other personal or social use of internet facilities must be kept to a minimum, and is only permitted between 8.30-9.00am and during lunch times.

Staff should not at any time access, or seek to access, websites which promote:

- sexually explicit material;
- violence;
- discrimination based on colour, age, marital status, gender, sexual orientation, race, belief, religion, disability, national or ethnic origin; or
- illegal activities or violations of intellectual property rights.

In addition, staff should not use the internet to:

- access streamed or real time audio, data, graphics, video or any other data which uses large amounts of bandwidth unless to access services directly related to their work; or
- download any information that is not directly related to their work.

E-mail usage

E-mail is routinely available to all staff through our computers.

The following guidance is given to ensure that the facility is properly used and not abused. If there is any doubt or concern, reference should be made to Miss Sidrah Butt, if a suspicious e-mail message is received, for example from an unidentifiable sender, especially with attachments, it should not be opened.

Particular caution is needed where the message is from a familiar source but there is no text in the message. In such circumstances please telephone the sender before opening that attachment to see if they have indeed sent a bona fide message to you. Alternatively, please refer the issue to Miss Sidrah Butt. Where there is still doubt, the message should be deleted without being opened.

The overriding principle is that e-mail messages are to be controlled and processed to the same standards as for normal correspondence. Because e-mails, both received and sent, are processed on an individual personal computer, in the majority of instances without the knowledge of the Directors there must inevitably be a high degree of trust from everyone in the use of e-mails.

The arrangements in relation to messages are as follows:

<u>Incoming messages</u>

- All incoming messages related to lettings must be printed out and a hard copy placed on the appropriate client file. A copy must also be saved on the electronic file and named appropriately to identify the sender and the date received.

<u>Outgoing messages</u>

- A printed copy of outgoing messages is to be placed on the relevant client file.
- A copy of the outgoing message is to be saved on the electronic file and named appropriately to identify the recipient and the date sent.
- No potentially offensive messages are to be sent. Defamation, harassment and breaches of our Equality & Diversity Policy are all potential risks. Please also be wary of the temptation to send off a hasty message that, on reflection, would seem unwise. A good rule is to place your initial response in your drafts folder or reply later or the next day if annoyed or offended by action taken or a communication received: allowing yourself a 'cooling-off period' can avoid putting yourself in the wrong.
- All e-mails are to be restricted to the Company's professional work.
- Always check the state of attachments to see that you are sending the correct draft. Be particularly wary of drafts that might have been amended without your knowledge by someone outside the Company – client, opponent or other. Where this is a risk, you should attach the document as a pdf that cannot be amended.

<u>Deletion of e-mails</u>

It is the responsibility of the individual to review regularly all stored messages and delete those that are no longer required. All staff members are asked to ensure that printed copies of messages, including draft documents, have been placed on the client file and saved to the electronic file before deletion of

messages.

Virus protection

The Company's e-mail facility is protected via our IT support providers and regular protection updates will be received.

Nobody may introduce to any PC any disc without the permission of the Directors. Failure to seek their permission before doing so will be treated as a disciplinary offence.

Responsibility for this policy lies with Miss Sidrah Butt who will review this annually.

E-mail & Internet Monitoring

We reserve the right to monitor all external and internal communication, user access controls and access to our network and internet where the property of the Company is used by staff members to include where it is accessed remotely from outside the Company. This includes laptops and mobile devices.

Miss Sidrah Butt is responsible for assessing the impact of any monitoring before it is introduced. Any assessment considers:

- the reason for implementing monitoring and whether it is justified;
- the likely adverse impact on employees and third parties communicating with the Company;
- the use of alternatives to monitoring or alternative methods of monitoring; and
- any additional obligations that arise as a result of the monitoring i.e. the secure storage of and access to information gathered by the monitoring.

In addition, she considers the impact of the monitoring on staff members, such as:

- the risk of intrusion into the staff members' private lives;
- the extent to which staff members will be aware of the monitoring;
- the impact monitoring will have on the relationship between staff members and the Company; and
- how monitoring will be perceived by staff members.

Miss Sidrah Butt will inform all members of staff prior to the introduction of any monitoring. Furthermore, she will inform individuals if their communications or internet access is specifically being monitored or accessed. However, an individual will not be informed where serious breaches of the policy or criminal activity is suspected and where informing the individual would hamper any investigation or risk the loss of data as evidence.

Miss Sidrah Butt, our DPO, is responsible for overseeing all monitoring.

Website Management Policy

This policy covers the website found at the following URL:

http://citylord.co.uk/

The website referred to is managed and operated by external developers. They handle, control and produce the website with content provided by us. All contributions, amendments and graphics / images are created by the external developers.

The materials contained on the above website are deemed to be for general information purposes only and do not constitute a contract. This Company does not accept any responsibility for any loss which may arise from accessing or relying upon information contained in this website.

Miss Sidrah Butt has responsibility for the management of the website including: -

- ensuring content is up to date;
- ensuring content does not infringe copyright;
- specifying conditions for downloading material;
- ensuring compliance with the Equality Act 2010;
- overseeing linking arrangements;
- ensuring posting of a privacy notice explaining how any data collected from visitors will be managed by the Company.

The Directors may delegate responsibility for inputting and maintaining the website however accountability for any content that is shown on the website remains with him.

Copyright and Trademark Notices
The contents of this site are protected by copyright under international law. Users are permitted to read the contents of our website and make copies of such content for their own personal use. They may also give copies to colleagues for their personal use on terms that City Lord Ltd is acknowledged as the source, the text is not altered in any way and the attention of the recipients is drawn to this warning. All other use and copying of any of the contents of this site is prohibited. Copying from websites of third parties is subject to any requirements applicable to those sites.

Accessibility
We are committed to making our website accessible for all our website visitors, including those with disabilities. We are committed to providing an accessible web service.

Data Protection
This Website is owned and operated by this Company, who is the 'Data Controller' for the purposes of the General Data Protection Regulations. This document is intended to explain how we use the information

we collect, how a client can instruct us if they prefer to limit the use of that information, and the procedures we have in place to safeguard their privacy.

Collection, Utilisation and Security of Data
Without limitation, any of the following Data may be collected:

- Name;
- Gender;
- Contact information such as email addresses and telephone numbers;
- Address and post code
- IP address (automatically collected);
- Web browser type and version (automatically collected by web analytics and traffic analysis software);
- Operating system (automatically collected by web analytics and traffic analysis software);

Our Use of Data
Any personal data will be retained by this Company for as long as the client needs access to the Services and Systems provided on the Web Site or the client has otherwise agreed to. Data the client may submit through any communications system that we may provide may be retained for a longer period of up to 6 years.

Unless we are obliged or permitted by law to do so, clients' Data will not be disclosed to third parties without their express permission. This includes our affiliates and / or other companies within our group.

All personal Data is stored securely in accordance with the principles of the General Data Protection Regulations.

Any or all of the above Data may be required by us from time to time in order to provide the client with the best possible service and experience when using our website. Specifically, Data may be used by us for the following reasons:

- internal record keeping
- improvement of our products / services
- transmission by email of promotional materials that may be of interest to the client
- contact for market research purposes which may be done using email, telephone, fax or mail. Such information may be used to customise or update the website

We use anonymous cookies to make the site as useful as possible. They are small text files we put in a user's browser to track usage of our site, but they don not tell us who the users are.

Compliance

Miss Sidrah Butt has overall responsibility for this policy and for monitoring compliance. She will carry out an annual review of the policy to verify it is in effective operation.