HODGSON COULTHARD & CO
SOLICITORS

Annex H

Information Management Policy

1. Introduction

This document sets out the firm's policies governing information risk management, data protection and data security. The policy aims to eliminate mismanagement of data which can result in serious consequences for the firm including significant fines under The General Data Protection Regulation, breaches of confidentiality and breaches of the SRA Code of Conduct. If any member of staff, regardless of their position or importance, fails to comply with this written policy they could be subject to the firm's disciplinary and grievance procedures which could ultimately result in dismissal. The purpose of the policy is to:

- Set out the various categories and types of data held at the firm
- Identifies the information storage assets
- Comply with the law
- Follow good practice
- Describe the roles and responsibilities of the different types of users in relation to the data
- Protect clients, staff and other individuals
- Protect the firm
- Comply with regulatory requirements
- Provide for the effective and efficient management of the firm's data, both in electronic and paper format

2. Responsibilities

The firm holds a huge amount of confidential information about clients, staff and third parties. We must all of us comply with data protection law and keep confidential information secure. Accordingly all staff must study and observe the precautions set out in this Policy.

The COLP is the firm's Data Protection Administrator as the nominated senior individual with overall responsibility for ensuring that the organisation complies with its legal obligations in relation to information management and data protection. This includes:

- Maintaining the firm's registration with the Information Commissioner.
- Ensuring the firm has good data protection procedures in place, including data security and staff training.
- Ensuring that any "subject access requests" which the firm receives from data subjects are properly handled.
- Reporting breaches of data protection where necessary.
- Approving contracts with data processors where appropriate

The firm is registered with the Information Commissioner's Office (ICO)**.** Renewal of the firm's registration or any amendments to it can be made via the internet, by telephone or by post. Further information can be obtained from the ICO website www.ico.org.uk or by telephoning 01625 545740. All details of the firm's registration are maintained by the Data Protection Officer.

3. General Data Protection Regulation (GDPR)

3.1 Overview

The GDPR governs the use of personal information by businesses and other organisations. It seeks to regulate how personal information is used and requires it to comply with their principles or rules of good information handling. The GDPR applies to personal information. Appropriate security measures must be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data. These include

both technical measures, e.g. data encryption and the regular backing-up of data files and organisational measures, e.g. staff data protection training.

GDPR states that when the firm holds information about identifiable people (known as "data subjects") this gives rise to obligations under the GDPR and applies whether such information is held in electronic form or in a paper filing system.

Data Subjects have rights if the firm holds information about them. These includes the right to be informed what the firm holds, the right to have errors corrected and the right to have data deleted if the form has no justification for holding it.

The firm may be liable in various ways if it fails to hold data appropriately. This may include liability in damages for negligence and breach of confidentiality or even criminal liability. The firm may also be subject to professional sanctions for breach of the SRA Code of Conduct.

3.2 Data protection principles

In processing personal data we must be able to demonstrate that we comply with the "data protection principles". These require that that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- kept with appropriate security.

3.3 Grounds for Processing Personal Data

The firm will only process personal data if we have a legitimate justification for doing so. Often the justification will be the consent of the person concerned. But note that in the case of someone under the age of 16 they cannot give that consent themselves and instead consent is required from a parent, or other person holding 'parental responsibility'.

Otherwise we may be entitled to proceed without consent on a number of grounds. Those which most often apply are the following:

- It is necessary for the performance of a contract to which the person concerned is a party.
- It is necessary for compliance with a legal obligation.
- It is necessary to protect someone's vital interests.
- It is necessary for our legitimate interests or those of a third party, except where such interests are overridden by the interests or rights of the person concerned.

3.3 Sensitive Personal Data

Sensitive personal data (referred to in the GDPR as "special categories of personal data") can only be processed under strict conditions. Sensitive personal data includes information about someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and sexual orientation, genetic data and biometric data. The usual grounds which entitle the firm to process such sensitive data are the following.

- Explicit consent of the data subject.
- It is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
- Data manifestly made public by the data subject.
- It is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

4 Information risk management

An annual review of this Policy will be undertaken The main risk to the firm is strategic with the loss of financial and client data through corruption, theft or system failure. However, loss of client data such as key dates and personnel information could affect the progression of individual cases. Also such loss could leave the firm in breach of their professional code of conduct rules as outlined by the SRA with regard to confidentiality and accounting rules. The review will ensure that all risks to information are identified and then assessed. At that point steps can be taken to mitigate the likelihood of the risk emerging and the impact of it should it occur. This will take place in conjunction with the firm's Business Continuity Plan (Annex D) it is believed that any impact on the firm will be over a short period.

5 Information Asset Register

A register of all the firm's client-related and firm-related information assets is set out in **Appendix 1** of this Policy. The great majority of the information assets are confidential. The firm takes care to protect confidential information applying the principles set out in this Policy.

The firm retains information for the periods set out in the Information Asset Register. These periods reflect the firm's data protection obligations not to keep personal data for longer than is necessary, and also with regard to statutory, regulatory and business needs to keep records. Thereafter information is disposed of securely, by shredding, electronic deletion, or otherwise as appropriate.

The data retention timescales will be subject to formal review at the Annual Quality Review as set out in QP01. Any amendments to timescales will be reflected in Appendix 1 and related documentation such as client care letters, terms and conditions of business etc.

6 Information management principles

The success of the firm depends on effective use of its information. It has therefore adopted the following information management principles.

(a) The firm's information is a corporate resource. All information belongs to the firm and not to any individual or group.
(b) Staff will limit colleagues' access to information they create or capture only if its sensitivity requires it.
(c) Staff will manage information consistently, including the use of approved naming conventions and filing structures.
(d) Staff will ensure that information is accurate and fit for purpose.
(e) Staff will retain or dispose of information appropriately.
(f) Staff will accept responsibility for the information they personally manage. Every member of staff is personally responsible for the effective management of the information they create, capture or use.
(g) Staff will manage information in compliance with statutory and regulatory requirements. In managing information, staff will comply with the relevant statutory and regulatory

requirements – including the requirement not to destroy information where there is a legal obligation to retain it.

The firm has the responsibility to train staff so that they can follow these principles. This is addressed by the induction process and annual review training to all staff.

7 Collection and distribution of data

7.1 Collection and use of data

Staff should not collect or use personal data without a good reason. If clients give us information about themselves this is rarely a problem, as they will usually expect us to record that information and use it for usual professional purposes. However take particular care with information about third parties, who may be unaware that we hold information about them.

Please bear in mind three simple principles:

- Do not record information about people unless you need to do so.
- Keep it secure.
- Delete it promptly when you no longer need it.
- Those principles apply especially to information of an embarrassing, secret or sensitive nature, and where the people concerned have not consented to us holding the information.

7.2 Distribution of data

Staff should take care when sending personal data to others. Staff will often need to share personal data and confidential information with others such as barristers, expert witnesses and other law firms. However, before doing so, the following should be considered:

- Do they really need the information?
- Should the firm redact documents so that they do not include irrelevant and unnecessary confidential information?
- Can the firm rely on the recipient to keep the information secure?
- Is the information being sent outside the European Economic Area? If so, check either that the country in question has been designated by the EU Commission as providing adequate data protection, or that the firm has appropriate contract clauses agreed with the recipient place to protect the data.
- In publications and publicity material all client identification information must be removed unless clients have consented.

8 Storage retention and disposal of information assets

Information is captured stored and maintained because it has a value to the organisation. Information that is inaccurate or out-of-date should not be kept (unless there is a clear historical value to the information). Indeed, keeping inaccurate information can be damaging. Staff should therefore aim to delete or destroy information appropriately that is no longer needed for business purposes and where there is no legal obligation to retain it.

9 Intellectual property of others (Copyright)

A document shall not incorporate the intellectual property of others unless the firm has the relevant rights. Staff will not enter documentation (including scanning) into an information system unless the

firm owns or has obtained the copyright to do so. Material specifically addressed to the firm can be entered into an information management system.

10 Confidentiality and the authorisation for disclosures

Confidentiality is covered within the firm's QPM (see QP02 and the firm's Client Care Policy (Annex C)) and outlines the circumstances under which confidentiality can be broken. This is in line with the SRA's guide to professional conduct. Within this policy we would extend the scope of that procedure to include data/information about the firm, its plans or finances. The firm is not allowed to use personal information for a reason an individual would not expect and is not allowed to pass an individual's information on to another business or organisation, unless they have asked that this be specifically done and the individual(s) have given their consent. Insofar as the firm is concerned the only time that there will be a transfer of information is when a file is transferred to another organisation or our files are audited by the accountants, SRA etc.

As indicated above, as far as the firm is concerned the only time that there will be a transfer/disclosure of information is when a file is transferred to another organisation or files are audited by the relevant bodies. Clearly though the Rule of Law allows exceptions for example if we were asked by the Police for information about someone, (clearly if not privileged), we can provide this information without notifying the individual, if notifying would likely to prejudice the investigation or impede the prevention or a crime. Clearly an example of this is money laundering notification. Disclosures can also be made if they are necessary for a Court case or to obtain legal advice for example, in connection with an employment tribunal.

11 Information security threats

11.1 Scope

Security must not be confused with confidentiality. The latter is about defining what is allowed - setting the boundary - the former is about ensuring that the boundary is maintained. However, there must be a relationship between the two. Information security covers not only electronic forms but also paper forms, whether handwritten or printed. In order to preserve security the firm needs to ensure maintenance of confidentiality, integrity and availability of such information. Compliance with these aims will allow use of the information with confidence. Such information and systems are at threat from internal and external sources

11.2 Types of threats

Physical: This results from either physical access to the systems from unauthorised personnel or damage to the components of the system i.e. computer terminals. It could also result from the computer equipment being stolen.

Electronic: These typically come from external sources and include hackers and viruses. Hackers gain control of computers primarily through the use of viruses that allow them to gain access to sensitive material which they can then copy alter or destroy. Alternatively websites can contain links that take you to other websites that copy your personal details by recording any key strokes that are made. Once infected a virus can be transferred from computer to computer through the use of external media such as USB drives. Virus is a term that incorporates Trojans and Worms into the definition.

Technical failure: If data is stored on only one computer, if that computer fails the data would be irretrievable. Hard disks will inevitably fail as they get older regardless of the expense of it.

Human Error: Misuse of a system, even if by way of an honest mistake, can result in information being lost. Security policies need to address human factors whether by a malicious outsider or an honest employee.

12 Information security measures

12.1 Backup of data

- To reduce any loss suffered by the practice if our IT security was breached, we back up all of our IT data on a regular basis to minimise the impact on the business. Backup routines are the responsibility of the firm's Bookkeeper. The firm has two external hard drives each of which is used to back up the server on a daily basis. One of the drives is kept on on-site and the other is maintained off-site by the Bookkeeper.
- In addition, a daily online backup of the server contents is conducted automatically to by the firm's IT Consultants Transcendit and stored on their secure servers.
- Due to the process used by backing up data, the risk posed when reinstating data is low.

12.2 Physical security of IT equipment

All computer terminals including mobile devices used for work purposes including phones, laptops and tablet computers must be closed down after use to prevent unauthorised use when the employee is not at their desk or in the office. All such devices must be password or security number protected so no-one can access the information stored or software installed on them without first entering the correct code.

Mobile devices used for work purposes including phones, laptops and tablet computers are stored out of sight when not in use by an employee. Staff should take all reasonable precautions to protect the physical security of such mobile devices, for example, they should use locked desks/cupboards/offices where available. Mobile devices must never be left unattended in cars at any time.

The computer terminals themselves are not physically accessible by anyone other than employees. At 10 Church Street, the file server is kept in the Bookkeeper's office which is kept locked when not attended and whose windows are protected by steel bars. The only access to clients and visitors is via the main entrance which is policed at all times by the Reception staff. Clients/visitors have to go through a further door past reception to physically enter the offices. A panic alarm is provided at Reception. The office is protected by intruder and fire alarms.

IT equipment must be thoroughly cleaned of information before disposal to ensure that no personal/sensitive data remains. Even if data has been deleted from electronic media it may be possible for others to recover it. Hence computer hard drives, data sticks, floppy disks, CD-ROMs etc. should either be cleaned by an expert or physically destroyed when no longer required.

12.3 Physical security of paper-based records

Staff should take all reasonable precautions to protect the physical security of client files and papers. Client files (or other confidential information) should only be taken out of the office when it is necessary to do so. Staff should take precautions to ensure that such items are not stolen or lost. For example, in no circumstances should files be left unattended in cars.

Confidential papers should be kept in locked cabinets when they are not in use. Staff should bear in mind that cleaning personnel, temporary staff and others may be present in the building, and that leaving papers where they can be seen risks a breach of security. Staff should report any stranger that they see in an entry-controlled area.

Staff should ensure that any work done on a client file on train journeys does remain confidential. Consideration should be given to who might overhear telephone calls on mobile phones in trains or in public places or view case papers/laptop screens etc.

All client files and other confidential papers are subject to confidential waste disposal when they reach their normal retention period.

HR records are kept in a locked cabinet.

12.4 Use of USB drives

The use of USB drives is restricted to those belonging to the firm. The firm holds a limited number of USB drives to be used by employees to transfer documents from one workstation to another. No personal USB drives are to be used by the employees. All other use of USB drives is strictly prohibited. Staff should take all reasonable precautions to protect the physical security of USB devices used for work purposes. For example, they should use locked desks/cupboards/offices where available. USB devices must never be left unattended in cars at any time.

12.5 Procedures for detecting and removing malicious software

It is the firm's policy that all computers, laptops and tablets have software installed on them that prevents, detects and removes malicious software. The software must be kept up to date at all times. All staff must immediately notify the IT Manager of any situation arising with the computers such as error messages or warnings of detection of potential malicious software who will then investigate and address the problem. Staff must not to open emails from suspicious sources or if they contain a suspicious attachment to minimise the risk of infecting the computer system. All emails from an anonymous sender are automatically treated as suspicious to minimise the risk of a virus.

Viruses are often contained in email attachments displayed as .exe or .scr. In order for the virus to infect the computer system the attachment has to be opened. Alternatively the virus can be picked up simply by visiting an infected website. Because of this, staff must be constantly vigilant to these risks when using the firm's equipment for email and internet access to reduce the chance of them containing harmful data that would infect the IT systems.

12.6 Preventing the misdirection of emails

Due to the risks from email, staff should observe the following precautions to avoid emails being misdirected:

- Consider whether the content of the email should be encrypted or password protected.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete

function may bring up several "Daves". Make sure you choose the right address before you click send.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Due to the severity of this risk employees are referred to the firm's Email and Internet Access Policy (Annex F)**.** Any breach of this could result in dismissal from the firm.

12.7 Preventing the misdirection of paper records

Care needs to be taken when sending paper records through the post or DX as serious breaches of data protection regulations can occur as a result of very simple errors. For example, take care to ensure that you check that enclosures are put into the correct envelope. Also, ensure that the correct enclosures are sent with covering letters. Particular caution needs to be taken when using shared printers as the wrong document can be picked up and placed in an envelope without checking.

Similarly caution should also be applied to the sending of fax messages. Staff should therefore take the following precautions:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if asked to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

12.8 Dealing with enquiries

Staff need to be aware of the existence of "blaggers" who are people who attempt to obtain confidential information by deception. This is most commonly done by phone but may also be by e-mail or by calling in person. The following are examples of the precautions you should take when dealing with enquiries.

- Check the identity of the person making the enquiry.
- Check we are authorised by the client (or other relevant person) to pass on this information.

- Ask callers to put their request in writing if you are not sure about the caller's identity and their identity cannot be checked.
- Refer to your supervisor for assistance in difficult situations.
- Take particular care with callers who claim to be from our bank. A number of firms have had money stolen from their bank accounts after staff gave confidential banking information out over the phone. Additional cybercrime prevention procedures are set out in QP12.

12.8 Use of firewalls

The firm maintains a firewall to prevent unauthorised access to the firm's network and data.

12.9 Procedures for the secure configuration of network devices

This is undertaken by our IT Support Company,

12.10 Management of user accounts

User accounts are managed by our IT Support Company. User accounts can be disabled at any time, for example on discovering a breach of security. Accounts are disabled when a member of staff leaves the firm.

Staff responsible for the management of payments (including fee earners and finance staff) are only recruited or assigned to that function after passing suitable background checks, including taking references and the verification of claimed qualifications.

Passwords are known only by staff members and are not written down. They are also changed on a regular basis to maintain privacy and the protection offered by a password.

13 Register of software

A register of all the software in use at the firm is held by our It Support Company. The maintenance of the Register is the responsibility of them. The register will be subject to annual review. This will take place in conjunction with the Annual Quality Review meeting arrangements set out in QP01. All software used by the firm is supported by external software suppliers who issue routine updates from time to time. It is the responsibility of the IT Support Company to decide whether and when updated versions are to be installed or new or better software should be obtained.

Staff should promptly update the software on their computer whenever required to do so. Updates frequently fix security weaknesses.

14 Subject Access Requests

14.1 General

A Subject Access Request is a request for personal information that the firm may hold about an individual. If an individual wishes to exercise their subject access right, the request must be made in writing. Under the GDPR, individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed;
- the description of the personal data concerning them;

- anyone who has received or will receive their personal data; and
- details of the origin of their data if it was not collected from them.

14.2 Fees

In most cases, the firm will be unable to charge the individual for the administrative costs of finding, gathering and disclosing data to the individual unless the individual's request is "manifestly unfounded or excessive". An example of the latter could be where a fee could be where a request is repetitive or if additional copies of the data are requested.

14.3 Procedure

The firm must respond to requests within **one month** of receipt. This deadline can be extended by a further two months where there are a number of requests or the request is complex but the individual must be contacted within a month of receipt explaining why the extension is necessary.

Staff must be alert to the possibility of the firm receiving a Subject Access Request. Because of the tight timescales involved all staff must respond immediately to any such requests. Staff with special responsibilities for receiving emails from the firm's generic email addresses must be particularly vigilant as requests can be made electronically. In the case of electronic requests, it is vital that the identity of the person seeking the information is verified before information is provided as the firm could, unwittingly, be facilitating a data breach.

All requests must be passed, without delay, to the COLP. If the COLP is not available then the request must be passed to a senior member of management. The COLP will be responsible for verifying the request and taking steps to provide the information in conjunction with other members of the firm, as appropriate. The deadline should be diarised to ensure compliance.

Where the firm holds a vast quantity of information about an individual, it may ask that individual to clarify what particular information they are referring to in the request. The organisation should then be able to consider whether the scale of the information requested is 'unfounded' and/or 'excessive' and react to the request accordingly.

All responses to requests must be authorised by the COLP or their nominated deputy.

14.4 Unfounded and excessive requests

In addition to being able to charge the individual if their request is unfounded and/or excessive, the firm may outright refuse to respond to the request. Only the COLP is able to authorise such a decision. In such cases, reasons for the refusal must be given to the individual. The individual will also need to be informed of their right to complain to the Information Commissioners Office and of their right to a judicial remedy. Both the reasons for refusal and the advising of the right to complain should be put to the individual without undue delay and, at the very latest, within one month of the request.

15 Data Protection Impact Assessments (DPIA)

15.1 General

DPIAs are a fundamental element of the GDPR and encourage organisations to adopt a 'privacy-by-design' approach when introducing a new data processing system or technology.

A DPIA helps organisations to find and fix problems at the early stages of any project, reducing the associated costs and damage to reputation that might otherwise accompany a data breach.

15.2 When is a DPIA required?

The firm must do a DPIA before it begins any type of processing which is "likely to result in a high risk to individuals' interests". This means that although the actual level of risk has not been assessed yet, the firm needs to screen for factors which point to the potential for a widespread or serious impact on individuals. In particular, the GDPR states that organisations must do a DPIA if they plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires organisations to do a DPIA if they plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

The risk assessment process is the responsibility of the Data Protection Administrator who will be responsible for undertaking the DPIA in accordance with this procedure for any projects deemed to be high risk.

15.3 Conducting the DPIA

The key stages in the development of a DPIA are as follows:

1	**Identify the need for the DPIA**	Determine whether the inherent risks of the processing operation require you to undertake a DPIA.
2	**Describe the information flow**	Describe how the information within the processing operation is collected, stored, used and deleted.
3	**Identify privacy and related risks**	Catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data you collect and/or process.
4	**Identify and evaluate privacy solutions**	for each identified risk to the personal data, make a 'risk decision', i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.
5	**Sign off and record the DPIA outcomes**	Record the outcomes of the DPIA (steps 1-4) in a report that is signed off by the Data Protection Administrator.

6	**Integrate the DPIA outcomes into the project plan**	Continually refer to the DPIA in order to ensure that it is being followed and that its responses to the risks have been implemented effectively.

The firm is not required to routinely submit DPIAs to the ICO. However, having carried out a DPIA that identifies a high risk, the firm cannot take any measures to reduce this risk then it must submit a report to the ICO and the firm cannot go ahead with the processing until it has done so.

16 Information security training

The firm ensures that all staff members are made fully aware of this policy and the specific requirements about information security risks and precautions. This is effected in a number of ways:

- Through the induction process;
- Considered at performance appraisals where any learning needs will be identified;
- Access to this Policy;
- Periodic updates at team meetings, one-to-ones and specific update training sessions.
- Periodic circulation of e-mails reminding staff of current criminal methodologies and risks as well as necessary precautions.

Appendix 1: Information Asset Register

No.	Asset Description	Media Type	Storage method	Key risks	Backup type	Lead responsibility	Retention period
1	Paper matter files (current)	Paper	Cabinets and shelving units	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	Heads of Department	During life of matter
2	Paper matter files (archived)	Paper	Cabinets and shelving units in archive store	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	Heads of Department	Minimum of 6 years
3	Client Due Diligence records	Paper	Stored on matter files (see above)	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	MLRO	6 years
4	Accounts records	Paper	Cabinets and shelving units	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	COFA	6 years
5	Personnel Records	Paper	Within locked cabinet drawers	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	Managing Partner	6 years after departure
6	Recruitment records	Paper	Within locked cabinet drawers	Fire/flood/theft/major incident	Paper matter file documents are also mostly available in electronic format	Managing Partner	12 months
7	Client database	Electronic	File server	Virus attack, IT failure	File server backup	IT Partner	20 years
8	General fee earner and	Electronic	File server	Virus attack, IT failure	File server backup	IT Partner	6 years

HODGSON COULTHARD & CO
SOLICITORS

Annex H

Information Management Policy

No.	Asset Description	Media Type	Storage method	Key risks	Backup type	Lead responsibility	Retention period
	miscellaneous computer documents						
9	Emails, calendars and user contacts)	Electronic	File server	Virus attack, IT failure	File server backup	IT Partner	6 years
10	Precedents and templates	Electronic	File server	Virus attack, IT failure	File server backup	IT Partner	6 years

Annex H

Information Management Policy