Purpose

This policy sets out the requirements to enable us to maintain the confidentiality, integrity and availability of client and other sensitive information when using the digital and physical resources supplied by the Firm and when using personal electronic devices

Scope

This policy covers all equipment and activities used to handle, store, transmit or move information in line with the Firm's Information Classification and Handling Process.

This includes, but is not limited to client information, financial information, information about members, employees, and consultants, new business ideas, marketing strategies, databases and computer/network access passwords.

This policy does not form part of contracts of employment. We may amend it at any time and decide to follow a different procedure where we consider it appropriate.

Responsibilities

The COLP has overall responsibility for this policy.
The Head of Compliance and the IT Director have operational responsibility for this policy.

Related documents

ITP01	IT Operations Policy
OPS15	Physical and environmental security policy
OPS22	Access control policy
ISMS06	Information Classification and Handling Process
CMF31	Visitor confidentiality agreement
ITA01	Password guideline document
HRP05	Disciplinary Procedure
Document	LLP agreement (Members only)
Application	ISO 27001 incident log

Affected teams

All teams

Related legislation / regulations

Computer Misuse Act 1990

Data Protection Act 2018

SRA Code of Conduct for Solicitors, paragraphs 6.3-6.5

SRA Code of Conduct for Firms, paragraphs 6.3-6.5

ISO27001:2013

1. Digital security – internal IT systems and equipment

IT systems are integral to the way that we work. In order to protect the information that we hold within our IT systems, we must put in place appropriate measures to mitigate the risks of information security incidents, as set out below.

It is important to recognise that all data that is passed through the Firm's systems will be stored and may be disclosable as part of a regulatory, client or Data Subject Access Request (DSAR). In addition, data may have to be disclosed as part of court and tribunal cases.

1.1. Password use

All systems in operational use across the Firm require a user name and password to allow appropriate access.

You **MUST**:

- Create strong passwords to prevent unauthorised access to the IT systems (see Password guideline document.)

You **MUST NOT**:

- Share passwords with anyone or write them down.

In the event that you forget your password, the IT Service Desk can issue a temporary password. At the first login you will be prompted to change the password which you must do immediately.

Passwords will expire after a predetermined period, with system reminders and additional notifications provided via Outlook.

1.2. E-mail usage

Using e-mail is a simple and effective method for communicating with others. To maintain the confidentiality of the information being sent, the following rules must be adhered to:

You **MUST**:

- Send and receive all work related e-mails using only the Firm's email system.
- Carefully consider the way that emails are written and take the same care as would be taken for any other communication, particularly when forwarding or when replying by email.
- Pause before sending emails – consider whether further reflection is necessary, and **never** send any communication which you would not read out in Court. Hastily giving advice increases the risk of making a mistake. Consider if the information is of a highly sensitive nature and send the information in line with the ISMS06 – Information Classification and Handling Process.
- Before sending an email, open all attachments and check them.
- Report any e-mails that are considered to be potentially harmful to the Firm immediately to the IT Service Desk and follow their instructions on how to deal with the e-mail.
- Report on the ISO 27001 incident log any emails that have been sent to the wrong recipient if data falls within the amber / red category in ISMS06 – Information Classification and Handling Process.
- Carefully consider whether to open emails which appear to be out of the ordinary.

You **MAY**:

- Use the Firm's e-mail system for personal use as long as it is kept to a minimum and is only used for legitimate and legal purposes, and so long as you only use your Shakespeare Martineau email address.

You **MUST NOT**:

- Open any attachments received from a suspicious or unknown email address.
- Send or receive any material that is obscene defamatory, or illegal in any other way.
- Send or receive any material which is intended to annoy, harass or intimidate another person.
- Represent personal opinions as those of the Firm.
- Send or forward any work related emails or attachments from your work email to your personal email.

- Download or save any work related information or attachments to personal devices for use outside of the Firm's business or operational purposes and without appropriate dispensation from the COLP or (in the COLP's absence) the IT Director.
- Use your personal email, e.g. Hotmail and Gmail, to carry out any work related matters and / or access such accounts through the Firm's systems without appropriate dispensation from the COLP or (in the COLP's absence) the IT Director.

1.3. Collaboration Tools for Business Usage

A number of collaboration capabilities exist across the Firm's landscape to support business operations, including Teams, Skype for Business, Zoom, etc to encourage and promote cohesive and effective working across the business. To maintain the confidentiality of the information being sent / viewed, the following rules must be adhered to:

You **MUST**:

- Carefully consider the way that 'Instant Messages' (IMs) and any information captured/ shared is written and take the same care as would be taken for any other communication, particularly when forwarding or when replying by IM. Please note that IM messages are stored centrally in the same way as emails.
- Report on the ISO 27001 incident log any information that has been sent to the wrong recipient if data falls within the amber / red category in ISMS06 – ISMS06 – Information Classification and Handling Process.
- Be mindful of data shown when sharing your screen in both internal and external meetings to ensure that no sensitive data is shown in error.

You **MUST NOT**:

- Send or receive any material that is obscene, defamatory or illegal in any other way.
- Send or receive any material which is intended to annoy, harass or intimidate another person.
- Send any sensitive data to people who should not have access to this data.
- Share information within online meetings that would breach our requirements to maintain client confidentiality, bearing in mind the attendees within the meeting.
- Represent personal opinions as those of the Firm.

1.4. Data rooms

Using data rooms can be an effective way to store and transfer files to and from clients. To maintain the confidentiality of the information being sent and received, the following rules must be adhered to:

You **MUST**:

- Complete the data room request form listing all users that are to have access to the data room and what permissions and folders they require access to.
- Report on the ISO 27001 incident log any instances of documents being uploaded to the wrong data room if data falls within the amber / red category in ISMS06 – ISMS06 – Information Classification and Handling Process
- Only upload data to the client's data room which is relevant to that client.
- Obtain you client's prior consent to using a data room.

You **MUST NOT**:

- Use the data room to store or share personal files to and from the firms IT systems to an external system.
- Use the data room to store, share or remove client or firm data from the firms IT systems to an external system.
- Give clients a single data room login for use by multiple users. All users who access the Data room must use their individual login details.
- Upload data which any third party with access to the data room is not permitted to see.

1.5. Internet usage

The Firm provides Internet access to assist you to carry out your day to day work activities. Websites that are not required for day to day business are blocked from access. If a blocked website is necessary for business purposes, a request can be sent to the IT Service Desk, to remove the block. To minimise the risk of a breach:

You **MUST**:

- Inform the IT Service Desk immediately of any unusual occurrences while accessing the internet e.g. you suspect that a website that you use has been fraudulently copied and does not look right.

You **MAY**:

- Use the Internet for personal use provided it is kept to a minimum and is for legitimate and legal purposes only.

You **MUST NOT**:

- Make unauthorised entry into any other computer or network via the Internet, or to disrupt or interfere with other computers or network users, services or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.
- Access nor seek to access parts of the Firm's systems which you do not have permission to access and / or have no legitimate reason to access.
- Deliberately transmit any virus, worm, Trojan horse or trap door program code into the Firm.
- View, download or transmit text or images which contain material that is:
  - Pornographic
  - Racist or politically extremist
  - Likely to incite violence or hatred
  - An illegal activity
  - Potentially offensive to other members of staff.

These offences are considered to be gross misconduct for staff under the Firm's disciplinary procedures and for Members under the terms of the LLP Agreement.

1.6. 3rd Party File Transfer Utilities

The use of 3rd Party file transfer utilities such as OneDrive, Google Docs and DropBox are often requested to support the transfer and interaction of documents and information between clients and SHMA staff. Access to these sites will be provided at the ongoing discretion of the IT director on a read only basis. Read only basis means that by default you must not (and will not be permitted to) upload information to such file transfer utilities.

Due to the constant change in file transfer utilities, maintaining access to an undefined list of "file transfer" type utilities would be impossible. In the event that the utility you wish to use is not one of those listed above and therefore inaccessible, please log a call with the IT Service Desk.

To maintain the security of the firms IT systems, the following rules must be adhered to when transferring files:

You **MUST**:

- Transfer documents back to the client using a firm provided file transfer facility or by email with any appropriate password and / or encryption.
- Only access the clients file transfer facility from a firm owned and supported workstation.

You **MUST NOT**:

- Open file transfer links in e-mails unless you know you are expecting specific requests to transfer files from the sender.

- Use file transfer facilities to transfer personal data, files or programs to the firms IT systems from an external system.
- Use your own hardware to access the clients file transfer facility.

Everyone does have access to OneDrive, for business operational use only. This should only be accessed with the user's Shakespeare Martineau login credentials.

1.7. Telephone use

Occasional personal calls are permitted during business hours as long as they are kept to a minimum, for legitimate and legal purposes only and calls are not outside of the UK (excessive use of the Firm's telephones for personal calls may result in the cost of the calls being reclaimed from you).

1.8. Printers, photocopiers, fax machines, scanners and cameras

It is important that printers, photocopiers, fax machines, scanners and cameras/photographic devices are used responsibly to prevent the inadvertent loss or circulation of sensitive information. The following measures will help to minimise these risks:

You **MUST** make reasonable efforts to:

- Collect your documents promptly and not leave them on the device where devices do not use Follow-Me print or similar technology.
- Ensure your printing is not interrupted part-way through meaning it is completed when you are not present at the machine (for example, if it runs out of paper and is later replenished by someone else).
- Make sure that documents are sent to the correct recipient.

You **MAY**:

- Seek permission from your Team Leader to utilise printers for personal use, as long as this is kept to a minimum and only used for legitimate and legal purposes.

You **MUST NOT**:

- Store, print or send information for illegitimate or illegal purposes.

2. Digital security – portable devices supplied by the Firm

Portable devices are provided for the purposes of communication and continuity when working away from desks. You must report lost devices immediately and return any broken or damaged devices to the IT team.

Mobile phones

Online storage services	The use of online storage services such as Dropbox and Google Docs is prohibited on all Firm provided mobile phones. The use of Microsoft OneDrive is permitted but only for business and operational purposes and must be accessed by using assigned Shakespeare Martineau credentials only.
Personal usage	Mobile phones are provided for business use as required. The Firm allows personal use of phones provided the use is kept to a minimum and is for legitimate and legal purposes only. Where it is considered that the usage is unacceptable the Firm reserves the right to ask the user to pay for the usage.
International calls	In the event that you travel abroad and wish to take your mobile phone with you, before travelling you **MUST** notify the IT Service Desk, who will provide advice regarding device compatibility with the destination and manage data roaming settings if required and notify our supplier. Please note our network provider **must** be notified in advance of travel abroad: if this is not done, extortionate roaming charges may be incurred, and we have been 'stung' before!
Security Abroad	Be minded that some countries can compel you to provide access to your telephone. If you are concerned (for example, re. travel to the USA) delete your Outlook and Mimecast apps prior to travel, reinstall them once through customs and security and remove them again before travelling home.
Driving	Government advice is that phones should be switched off when driving and we would recommend that you follow the advice provided.
Special requirements	There are areas within our offices where clients have specific requirements relating to the restricted use of mobile phones. If you are working in such an area, your Team Leader will inform you of any specific requirements that relate to you.

2.1. Laptops and tablets

Online storage services	The use of online storage services such as Dropbox and Google Docs is prohibited on all Firm provided mobile phones. The use of Microsoft OneDrive is permitted but only for business and operational purposes and must be accessed by using assigned Shakespeare Martineau credentials only.
Personal usage	The Firm allows personal use of devices, provided the use is kept to a minimum and outside of core working hours and is for legitimate and legal purposes only. Further, no personal documents may be saved on such devices.
Software	Software may be downloaded onto equipment owned by the Firm, without authorisation from the IT Service Desk as long as it is appropriate and for productivity purposes. A SHMA portal exists for most business applications in use across the firm and this provides an "approved" list of all applications in use. Anything outside of the portal should be considered carefully before being downloaded. If you are unsure, please contact the IT technical services manager or IT Service Desk before downloading.

Saving to your Firm laptop	The Firm's devices are configured to allow local availability of information/ documents to facilitate off-line working. Appropriate care should be taken when saving anything to the device to ensure it is appropriate for business and operational use.

2.2. Removable media

Memory sticks	USB ports are limited to read only unless a firm-provided encrypted device is used with a specific firm-assured password capability, to prevent unauthorised introduction or removal of information to and from the IT system. Encrypted memory sticks can be used, where necessary, with support from the IT Service Desk (which must be obtained).
CD / DVD (Optical media)	When providing confidential information to a client using CD / DVD, the information must be encrypted and the encryption codes sent separately to the client. As an alternative, users should try to encourage use of Data Rooms for these purposes.

3. Digital security – personal portable devices

3.1. Mobile phones

Personal mobile phones	The Firm allows the use of personal mobile phones for personal use, provided the use is kept to a minimum, does not interfere with your work and is for legitimate and legal purposes only (and does not breach any client imposed restrictions relevant to your area of work).
Voicemail, text and instant messages	The Firm **does not** allow work related information to be sent to personal mobile phones in the form of voicemail, text or any other instant messages unless dispensation has been provided by the COLP or (in the COLP's absence) the IT Director.

3.2. Laptops and tablets

Personal laptops and tablets	The Firm allows use of personal laptops and tablets, provided the use is kept to a minimum, does not interfere with your work and is for legitimate and legal purposes only.

3.3. Remote Access - (Use Your Own Device)

This section sets out the use of devices for remote access to the Firm's IT systems via Citrix. Anyone accessing the Firm's IT system remotely through an SHMA controlled device using Mobile Device Management (section 3.4) will remain unaffected by the policies in this section.

Any type of personal home devices (Wintel or Apple Mac) which are used for remote access to the Firm's IT systems using Citrix, or a secure EUC build in some instances, must be malware and infection free.

The following measures will help to minimise any risks to the individual and SHMA:

You MUST:

- Download and install the latest security updates for your personal/ home device.
- Use an IT approved commercially available anti-virus product (See list of approved Antivirus Products) which is a current version and has up-to-date definitions.
- Inform the IT Service Desk at the first opportunity if your personal/ home device is lost, stolen or compromised in any way.

You MUST NOT:

- Download or save any work related information or attachments to your personal/ home device.
- Transfer work related information from removable media (e.g. USB and CD) to personal portable devices.
- Print any work related information to a personal printer.

The Firm accepts no responsibility for the loss of personal information or damage that may be caused when accessing the Firm's systems from any "use your own" device.

List of approved Antivirus Products

Recommended:- Norton AntiVirus/Security, McAfee, Kaspersky.

Free Antivirus Products that are acceptable:- Sophos, Microsoft Windows Defender, AVG.

3.4. Mobile device management - (Bring Your Own Device - BYOD)

This section sets out the use of personal portable devices for remote access to the Firm's IT systems which are **outside** of Citrix. Anyone accessing the Firm's IT system remotely through the Citrix system will remain unaffected by the policies in this section.

Any type of personal portable devices which are used for remote access to the Firm's IT systems **outside** of Citrix (e.g. WebMail, BigHand, Mimecast) must be configured with the Firm's mobile device management application and an accompanying 'Personal MDM Mobile Device Management Waiver' signed by the user. At no point will the Firm have access to your personal device or its data.

The Firm's mobile device management application will be downloaded to the device and will enforce the need to set a password of at least 4 digits on the device and the device will automatically lock after 1 minute of inactivity. If the password is entered incorrectly 5 times, the device will be reset to factory settings with all information on the device deleted.

If you lose your device, you must inform the IT Service Desk who will then remotely wipe your device which will result in a loss of all device data, both Firm and personal.

If you leave the Firm or replace the device, you will need to contact the IT Service Desk so that the application can be removed. Failure to do so will result in a remote wipe taking place to remove any confidential information that may still be on the device, which will result in a loss of all device data, both Firm and personal.

The Firm accepts no responsibility for the loss of personal information or damage that may be caused when accessing the Firm's systems from the device.

The following measures will help to minimise these risks:

You **MUST**:

- Obtain approval from your Team Leader to use personal portable devices to access the Firm's IT systems outside of Citrix e.g. Webmail, BigHand and Mimecast, and sign the 'Personal MDM Mobile Device Management Waiver'.

  (Please note Webmail is no longer being installed on personal portable devices).

- Inform the IT Service Desk at the first opportunity if you lose your personal portable device.
- Contact the IT Service Desk at the first opportunity if you are leaving the Firm or replacing your device.

You **MUST NOT**:

- Download or save any work related information or attachments to personal portable devices, outside of the Firm's Citrix environment.
- Transfer work related information from removable media (e.g. USB and CD) to personal portable devices.
- Print any work related information to a personal printer unless authorised to do so by the COLP.

4. Physical security

Information security incidents can occur where there is a loss of, theft of or unauthorised access to physical information e.g. client files / papers. The key expectations for maintaining effective physical security are set out below:

4.1. Entering and leaving offices

The way that we enter and leave offices can create opportunities for security breaches. For example, an activity known as "tailgating" is where an unauthorised person follows another person to gain access whilst a secure door is open. To minimise the risk of an incident:

You **MUST**:

- Use the appropriate security pass or code issued to you when entering a secured door and keep this security pass or code secure at all time.
- Make the best effort to ensure that no-one has entered the secure door that you do not recognise.
- Politely challenge anyone that you do not recognise and report anyone who is trying to gain unauthorised access.
- Report a lost or stolen pass or code to the Facilities team immediately.

You **MAY**:

- Allow access to someone that you know has the right to access the area.

You **MUST NOT**:

- Allow someone access, unless you are satisfied that they have a legitimate right to be there.
- Wedge doors open.
- Provide your security pass or code to other individuals.

4.2. Visitors and unknown people

A simple way to access information without authorisation is to confidently move around an office as if you belong there. It is therefore important for us all to make sure that people in and around our work areas have a legitimate need to be there. To minimise the risk of an incident:

You **MUST**:

- Politely challenge anyone in your work area that you do not recognise
- Report all instances where a challenge establishes that the person should not be where they are.
- Ask for help if the person being challenged is aggressive and unhelpful.

You **MAY**:

- Ask for support in challenging a person if you do not feel confident to do it alone.

You **MUST NOT**:

- Be rude or aggressive when challenging someone in your area that you do not recognise
- Be rude or aggressive when being challenged by someone in a work area.

If you are expecting a visitor who requires access to a work area, you must complete and sign the Visitor Confidentiality Agreement (CMF31) prior to accessing the work area and return to the Risk Team. Physical copies of this form are also available from each office reception area. If any visitors also require sight of or access to our IT system, you must consult with the Risk Team prior to the visit.

4.3. Clear desks

Information left on desks is reasonably secured as our office areas are protected through secure access control systems. This does not eliminate risks associated with information security as people have unescorted access to these environments, especially out of hours, such as cleaners, building management staff and maintenance workers. For this reason care still needs to be taken around physical information in these areas, in accordance with our ISMS06 – Information Classification and Handling Process. To minimise the risk of an incident:

You **MUST** make reasonable efforts to:

- Conceal sensitive information when you are away from your desk – all users must use the lockers and appropriate storage for these purposes.
- Clear your desk of any sensitive information and all personal items at the end of each working day.
- Maintain a controlled working environment.

You **MAY**:

- Leave closed files in storage locations such as bookcases or roller racking assigned to you/ your team.
-

You **MUST NOT**:

- Leave files in meeting rooms (on working floors or within Reception areas) or unsecure areas within the office.

4.4. Clear screens

Computer screens can be read or systems accessed just as easily as physical information. For this reason it is important to secure computers when not in use. To minimise the risk of a breach:

You **MUST** make reasonable efforts to:

- Lock your computer when you are out of sight of your desk. This can be done by simultaneously pressing the 'Windows' key and the letter 'L'.
- Logout from the computer you are using when you leave the office for the day.

You **MAY**:

- Minimise your screen if you are in sight of your desk.
- Ask people to move away from your desk to protect the confidentiality of information if you are working on sensitive information.

You **MUST NOT**:

- Leave sensitive information visible on your screen when you are away from your desk, even if the screen is still in your sight.

4.5. Remote working

The Firm recognises that it is not possible to completely eliminate the need to remove information from the offices, however precautions must be made to ensure that access to and confidentiality of client information and sensitive Firm information is maintained. To minimise the risk of a breach if you are taking papers out of the office (to include taking papers to Court or to an off-site Client visit):

You **MUST**:

- Client Information, sensitive Firm information and original documents:
  - Have authorisation from your Supervisor/Line Manager to take documents of this nature outside of the office;
  - Make a suitably named electronic record of the authorisation (e.g. a file note or email) on the case plan/document management system used by your team which is sufficient to allow you to know what was removed in the event of loss.
- All documents which are not Client Information, sensitive Firm information or original documents:
  - Make a suitably named electronic record (e.g. a file note or email) on the case plan/document management system used by your team which is sufficient to allow you to know what was removed in the event of loss.
- **ALL** documents:
  - Only take essential information for the specific period that you are away from the office (e.g. there is unlikely to be a need to remove billing records/client ID/ commercially sensitive information from the office. Guidance around this may be adjusted based on external circumstances, e.g. COVID 19.
  - Make sure information is secure at all times during transit.
  - Be conscious of your environment when viewing / discussing client or Firm sensitive information to prevent any inadvertent information loss or circulation.

You **MUST NOT**:

- Leave files or equipment unattended in public places, in cars overnight or other unsecure places.
- Work on, or discuss, sensitive information in public places, e.g. restaurants or whilst travelling on public transport.
- (other than in extremis) take original documents out of the office.

5. Reporting incidents

Where an incident has been observed that represents a breach of the terms of this policy or may represent an actual or potential security breach it is important to record the incident on the ISO 27001 incident log.

If you identify an information security weakness or incident, you **MUST**:

- report it to the IT Service Desk as soon as possible and
- record the details on the ISO 27001 incident log (accessed via the intranet).

The Risk Team will use this information to identify improvement opportunities for the Firm to improve the effectiveness of our information security. Some incidents may require an entry on our SRA rules breach register (and sometimes reporting to the SRA).

6. Monitoring compliance with this policy

The Firm reserves the right to monitor all content stored and passed through the systems to monitor for compliance with the requirements of this policy. This will apply to business and personal information stored or transmitted via the Firm's systems.

7. Training

All staff must be aware of and adhere to this policy. General training is provided at induction, through completion of online Data Protection Training and Information Security modules and through periodic risk awareness training.

8. Non-compliance with this policy

Any concerns with adherence to this policy must be reported to the Risk Team.

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Firm's Disciplinary Procedure (or for Members, any actions resulting in a breach of the obligations under the terms of the LLP agreement may result in action being taken by the Firm's Members Board).

Depending on the seriousness of the offence, it may amount to gross misconduct and could result in your summary dismissal i.e. termination of your employment without notice.

9. Policy review

The policy will be reviewed as part of our periodic review process, based on the criteria below:

- Major changes in the law or practice.
- We identify or are alerted to a weakness in the policy.
- Changes in the nature of our business, our clients or other changes which impact on this policy.
- At least annually.