Information Security Policy

Context and overview

Policy prepared by: Scott Baldwin

Approved by Management Committee on: 15/10/2018

Policy became operational on: 10/11/2018

This Policy will be reviewed on an Annual basis or in line with any regulatory changes.

Last Review Date: N/A

Next review date: 3/10/2019

Introduction

St. Mary's Chambers needs to gather and use personal and sensitive information about individuals.

This includes data from clients, suppliers, Chambers contacts, employees, pupils, members and other people we have a relationship with or may need to contact.

There is a risk involved whenever data is collected, stored and used and this policy sets out our approach to the security measures we put in place to protect the data we collect, store and use in all aspects of our Chambers.

Why this policy exists

St. Mary's Chambers is a barristers' chambers which specialises in family law. In the course of providing legal services to professional and lay clients we use court bundles and supplementary materials which contain highly sensitive data about individuals. This includes medical, police, court and social work records. It can also include financial matters including details of bank accounts, investments, pensions, properties, debts etc. Some of the individuals involved in the cases in which we are instructed are highly vulnerable and the impact of data being improperly used or disclosed could, in the most extreme cases, lead to death or serious injury.

In order to provide legal services to our clients the data we use has to be transported from one location to another for the preparation of cases and in the provision of advocacy and advisory services at court and other locations. The data we use can be in electronic and hard copy format and there are specific security risks with both types of data. We take information security seriously and look to build in appropriate security measures to every aspect of our Chambers.

It is important to us that not only do we safeguard our data for the reasons detailed above but also to ensure we can protect the rights of individuals, be open and transparent about what we do with your information and put your mind at ease that your data is in safe hands.

Risk assessment

In preparing this policy we undertook an information security risk assessment. This helped to clarify our thinking in assessing the most severe impacts were our data security measures to fail. We determined that the highest risks and most severe impacts centred around the data contained in the briefs and court bundles that our barristers use to provide their services. This then provided our focus in designing our security measures to ensure that we do all that we reasonably can to protect all of the data we handle.

Access Controls

Case data

The staff have access to all the case data for all the barristers. The staff provide administrative support to the barristers by managing their diaries, processing incoming data, invoicing and credit control and therefore need access to all the case data to fulfil their roles. The staff record and distribute all the case data to the appropriate barrister.

Each barrister only has access to case data relating to their own case load. If this were not the case, there would be a risk that a barrister did see case data for a client who they did not act for then they could become conflicted and be unable to act for any of the parties. In the event of a complaint from a client relating to the service provided by a barrister the case data for that case would need to be provided to a member of the Complaints Committee for a formal investigation to take place.

Personnel data

Data relating to personnel is only available to those who need it for a specific purpose. In general, the Management Committee have access to all data relating to personnel as they are responsible for all aspects of managing the administration of Chambers. Unless there is a good reason to disclose data relating to staff to all members of Chambers, the Management Committee would normally be the only people to use such data. If this was to be released, the reason would have to be justified and you would be informed of this disclosure should a decision to do so be made. The obvious exception would be where a new member of staff is being recruited and pertinent details of a successful applicant would be provided to all tenants and staff.

The Management Committee delegate some of their responsibilities to other committees:

The Pupillage Committee handle all aspects of the recruitment and training of pupils.
The Recruitment Committee handle all aspects of considering applications for tenancy from established practitioners.

These sub-committees process data relating to many applicants, many of whom do not fit the criteria of our recruitment policy and therefore the data relating to unsuccessful applicants is not disclosed outside these committees. It is only when an applicant is recommended to Chambers to be offered a pupillage or tenancy that the data would be possibly be disclosed to the other tenants of Chambers. Any data collected as part of the recruitment process will be stored in accordance with our data retention procedure detailed below in the "Data Retention" section.

Chambers data

Each individual member of Chambers is jointly and severally liable for all Chambers expenditure. As such each tenant is allowed access to any data which relates to the accounts and bookkeeping of St. Mary's Chambers. It does not allow them access to the Chambers and financial data relating to each individual barrister. The Senior Clerk and Fees Administrator both use the Chambers data to assist in the running of Chambers. The rest of the staff do not have access to the Chambers data.

Physical Security

The main entrance to Chambers is through a door which is locked outside of normal office hours. There is then a second door through which access is controlled by a control panel which requires a four-digit pass code to allow access or else to use an intercom to seek access to be granted. There is also a back door to Chambers which is accessed through a security gate through which access is controlled by a control panel which requires a four-digit pass code. These passcodes for both doors are changed on an annual basis and this information is provided to employees, pupils and members of Chambers on a need to know basis.

There are four CCTV security cameras which cover the main front security doors, the reception area, the alley way accessed through the rear security gate and the back door. The CCTV is clearly signed upon entrance to the Chambers, recordings of the CCTV are retained for three months which can be accessed by the data protection officer and deleted after the outlined timeframe. Chambers has an intruder alarm which is armed when the building is empty outside normal office hours. Access to the building is therefore restricted only to those who should have access.

There are occasions where external contractors require access to the building outside of normal hours. When this occurs, access is only granted for a clearly defined period and purpose, all client data will be appropriately secured away whilst this access is granted and any offices where access is not required will be locked in order to secure the data held. Once this period of time is over and access is no longer required, the door codes are changed immediately.

Network Security

All of our servers are hosted in the cloud. The data centre is run by a company named Supportstack who also provide the bulk of our IT support. They are ISO 27001 certified and have policies and procedures in place which cover the following:

- Physical security
- Strict management processes
- Cyber security
- CCTV
- Strict HR policies
- Restricted entry

These Policies can be accessed by contacting help@supportstack.com .

Our IT support company ensure that software security updates are applied as soon as they become available, backups are taken of our data on a twice daily basis and there is sufficient resilience built into their hardware to ensure Chambers continuity.

Access to the servers is primarily through thin client terminals and so no data can be stored on site without the use of an external memory storage device which is provided by IT and is securely encrypted. This assists in preventing accidental downloading and storage of data.

Each individual user has a unique login and password to access the server. Each user also needs another login and password to access our database and case management software.

Email and internet use

Permitted and prohibited use of email

Email is available to all employees, pupils and members of Chambers through the Chambers' computer network and is used to assist with day-to-day Chambers activities.

Personal use of the Chambers' email facility is acceptable provided:

- The use is minimal and mainly outside of working hours i.e. during lunch breaks;
- The use does not interfere with client or Chambers commitments;
- Usage complies with all other related Chambers' policies

Care should be taken to use the same standard of language and format that you would use in a letter. Remember that emails can quite easily find their way into the public domain and therefore you must not include any content which could cause offence to the reader of embarrass the Chambers. It is important to remember that emails from the Chambers have the same legal effect as a letter.

You must not send any abusive, obscene, sexist, racist, harassing or defamatory messages. If you receive such a message, do not forward it on to anybody else, report it to the Data Protection Officer. Chambers will take appropriate measures to remedy any breach of this policy through the relevant framework in place.

All employees, pupils and members of Chambers must refrain from sending hasty emails that on reflection would seem unwise. If you are annoyed or offended by an email that you receive, you should allow yourself a 'cooling off period' before responding.

Copyright

Copyright work must not be sent by email without the consent of the owner of the work. Copying and pasting material from the internet or other emails may infringe copyright and care must be taken to ensure that such material is not copied by email.

Out of office messages

Out of office messages must be set if a member of staff is away from Chambers for half a day or more. Staff must provide contact details for alternative members of staff for urgent messages.

Pupils and members of Chambers must set an out of office message when on leave, asking the sender to contact the clerks if a response is required prior to their return.

Social Media

Introduction

Social media is now widely used in today's society and is increasingly used by many of our clients and other professionals. It is therefore important that we embrace social media as part of our working practices to engage with our clients and to network with other professionals. However, there are risks with using social media if it is not used professionally.

Purpose

This policy aims to explain how the Chambers expects social media to be used by its employees, pupils and members and any other parties working on behalf of the Chambers.

Scope

This policy applies to all employees, pupils, members of Chambers, consultants and any third party that this policy has been communicated to.

The rules communicated in this policy apply to the use of social media:

During and out of office hours;
Whether accessed using the Chambers' IT equipment or equipment belonging to an individual.

Responsibility

The Data Protection Officer is responsible for this policy and for monitoring the Chambers' compliance with this policy.

Everyone in the Chambers (and any third party to whom this policy applies to) is responsible for ensuring that they comply with this policy.

Chambers will take appropriate measures to remedy any breach of the Clear Desk Policy through the relevant framework in place.

What is social media?

Social media are web-based technologies that turn communication into active dialogue. Examples of social media include:

Social networking websites such as Facebook, LinkedIn and Legal OnRamp;
Micro-blogging sites such as Twitter;
Web blogs;
Forums and comment spaces on information-based websites i.e. BBC Have Your Say;
Video and photo sharing websites such as Flickr and YouTube;
Forums and discussions boards; and
Any other website that allows individual users to use publishing tools.

Participating in social media on behalf of the Chambers

Chambers uses social media in accordance with its Marketing Plan to raise awareness of the Chambers and support the Chambers objectives.

The Data Protection Officer manages the Chambers' social media accounts on behalf of Chambers. No other person is authorised to use Chambers' social media accounts without the Data Protection Officer's express approval.

However, everyone has a role to play in protecting the Chambers' reputation and therefore if you see a posting which is incorrect or reflects badly on Chambers, you should report it to the Data Protection Officer immediately.

Permitted and prohibited use of social media

When using social media for Chambers purposes, all employees, pupils, members of Chambers and any other person(s) to whom this policy applies must:

Never use social media to make defamatory or damaging comments about Chambers, colleagues, other professionals or anybody associated with Chambers including clients;
Ensure that use of social media does not breach Chambers' policies on confidentiality, equality & diversity, data protection or any other relevant policy;
Never disclose any work-related issue or material that could identify an individual who is a client or colleague, which could adversely affect Chambers or a client;
Never suggest that any views expressed on social media are the views or opinions of Chambers;
Use Chambers' logo, brand names, trademarks and colour schemes in line with Chambers protocols; and
Ensure that they do not breach any copyright or intellectual property rights of others.

Security of social media accounts

Chambers expects everybody using social media accounts for Chambers purposes to ensure that they review their privacy settings and ensure that appropriate restrictions are in place on who can access Chambers information. However, it is accepted that adopting privacy settings does not always protect information posted as some sites are completely open to the public.

Personal use of social media (for non-Chambers purposes)

Employees, pupils and members of Chambers must continue to observe the Chambers' rules around social media when using their personal social media accounts for non-Chambers purposes.

Chambers will take appropriate measures if any comments or behaviour made via social media are deemed unfavourable to Chambers or its clients through the relevant framework in place.

Storage and maintenance

Data Groups

For the purposes of data management we have allocated the data that we collect and store into one of the following groups:

Data Group	Description
Brief – Digital	Details relating to the case about the party we act for and other parties in the case. Includes instructions, court bundle, correspondence and related documents all in digital format.
Brief – Paper	Details relating to the case about the party we act for and other parties in the case. Includes instructions, court bundle, correspondence and related documents all in hard copy.
Case Records	Records of each case including contact details, diary management, key case documents, billing and payment information.
Contact Details – Chambers	Contact details relating to barristers, members of staff, pupils and suppliers of goods/services.
Contact Details – Marketing	Contact details for professional clients.
Contact Details – Third Parties	Contact details for other parties involved in cases. Barristers and clerks from other chambers. Courts, judges and court staff. Litigants in person etc
E-mails – Clients	E-mails to and from clients which can include case files and correspondence relating to cases.
E-mails – Chambers	E-mails relating to the running of Chambers which can include financial and personal information.
E-mails – Third Parties	E-mails between other parties involved in cases. Barristers and clerks from other chambers. Courts, judges and court staff. Litigants in person etc
Financial Information – Chambers	Bank details to allow payments to staff, pupils, barristers and Chambers suppliers of goods and services. Accounts relating to the running of Chambers.
HR	Records relating to current and past members of staff, pupils and barristers
Recruitment	Personal details relating to recruitment of staff, barristers and pupils.

Each data group has different characteristics and so each is managed differently, however all data groups are handled with the same level of security.

Data Audits

We audit all the data we hold at least once a year to check whether it is still required and where it is to be retained we also check it is accurate. Much of the data we hold can be deleted or removed from regular use via automated systems. The Data Protection Officer oversees all auditing to ensure it is performed regularly and in line with our policies and procedures.

The data groups set out above share some common features and use the same IT and physical storage solutions and so for the purpose of auditing can be grouped together.

Brief – Digital, Case Records

This data is stored in LEX and Sharefile. LEX can be set up to create automatic reminders to delete any data which is no longer required within those parameters. LEX integrates with Sharefile and so any associated data can be deleted at the same time. We have set the automatic reminders to activate in line with our retention policy.

Brief – Paper

This data is stored on allocated shelves in the appropriate barrister's room. Once a quarter we perform an audit of each shelf and remove any hard copy documents which relate to cases which have concluded or for which we have no future part to play. The papers are either returned to the client or securely shredded.

Contact Details – Chambers, Marketing & Third Parties

For the most part this data is kept up to date through continual use. We use it to communicate with on a regular basis and any changes are normally made as soon as we are aware. Our case management software has a feature which allows us to get in contact with anyone on our database and ask them to update their contact details. This includes an opt in/out for all e-mails not directly connected with cases: social events, marketing, legal updates etc. This will be used to perform an annual audit firstly to check contact details are correct and for marketing contacts to check they still wish to receive communications from us which are not directly related to cases.

E-Mails – Clients, Chambers & Third Parties

This data is managed through Office 365 and Exchange. Automated archiving can be set up to archive, put beyond use and eventually delete e-mails at set intervals. The archiving policies are set up in line with our retention policy.

Financial Information – Chambers

For the most part this data is kept up to date through continual use. We use it to make payments to staff, pupils, members and suppliers on a regular basis and therefore rely on those we make payments to, to inform us if their bank details change. When someone leaves Chambers their details are deleted from our records on the next monthly payment run. For third party suppliers we store their details on RBS online banking as regular payees. We audit these

payees on an annual basis and delete any which have had no payments in the last two years.

Recruitment, HR

The Management, Pupillage and Recruitment Committees are responsible for processing the data relating to recruitment & HR. Each committee is reminded annually that an audit should take place of all data they currently hold. They then report back to the Data Protection Officer to confirm that an audit has taken place and data has been deleted or updated as appropriate.

Retention Policies

Brief – Digital, Paper

Most of our instructions come from professional clients and the briefs are always copies of originals and so can be securely disposed of as soon as the case concludes or else our involvement is no longer required. We also receive briefs direct from lay clients through the Public Access scheme. In such cases we have no professional client to refer to and therefore cannot be sure of the archiving and record keeping of the client. We therefore retain such data for seven years after the conclusion of the case and thereafter return the brief or securely destroy it as required by the client.

Case Record

Case records contain all the information required in the administration of each case. This includes contact details for the professional client, dates of court hearings and other appointments, details of the barristers' fees, copies of instructions and copies of key documents relating to the case. Some of the key documents are those we produce ourselves when communicating with the client, produced by the barrister as part of the legal procedure or retained solely for the purpose of claiming fees in publicly funded cases from the Legal Aid Agency. We normally retain this data for seven years after the conclusion of the case. There are a few exceptions to this rule. In cases where we represent the child we must retain the data for seven years after the child reaches majority. In cases which are publicly funded we must retain data for seven years after the instructing solicitor submits their final bill. When the appropriate retention period expires the data is deleted from LEX. After our involvement in a case has ended and prior to deletion of the case, the case record will be archived which puts it beyond normal use. Access to archived case records is available on request from the Data Protection Officer.

Contact Details

Names and contact details will be stored indefinitely or until Chambers becomes aware or is informed that the individual has ceased to be a potential client/supplier.

E-mails

Office 365 via hosted Exchange has an automated archiving system. We have therefore set this to routinely archive e-mails after 6 months, then after 2 years the e-mails are put beyond regular use before finally being deleted after 7 years. Access to e-mails put beyond use is on available on request from the Data Protection Officer.

Financial Data – Chambers

Hard copies of all documents relating to Chambers accounts are retained for seven years.

Recruitment, HR

Data relating to recruitment is retained for two years and then is securely disposed of in line with our policies. Data relating to HR issues is retained for two years after the departure of the clerk, pupil or tenant unless there is some ongoing issue which necessitates longer retention.

Disposal

Data is stored in three ways: paper/hard copy, digitally on hosted servers and digitally on removable media.

Data held in hard copy format is disposed of using a secure shredding facility provided by Shred-Pro. They provide locked cabinets which are located in various location around Chambers. Documents can be posted into these cabinets and they are collected and shredded on site every two weeks.

Data held digitally on the hosted servers can be deleted in the normal way. Automated clean up of recycle bins have been set up to ensure digital data is completely removed.

Data held on removable devices is disposed of by S2S Group who collect and securely destroy such media. Upon destruction we receive certification of secure disposal.

Security breach/incident management

Our responsibility

In Chambers, we are responsible for ensuring that personal data processed by Chambers is not:

- Accessed without authority;
- Processed unlawfully;
- Lost;
- Destroyed; or
- Damaged.

Nevertheless, we realise that from time-to-time things may go wrong and we might fail to achieve one or more of our data protection responsibilities.

If this does happen, it is essential that we take steps to try and put things right. However, we can only do this if we know that there has been a problem.

Therefore, everybody in this Chambers has a duty to report any actual or suspected data breaches, regardless of whether they have discovered them or have caused them.

What is a data protection breach?

A data protection breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Data protection breaches can happen for a wide range of reasons, including:

Human error;
Cyber-attacks;
Loss or theft of devices or equipment on which personal data is stored;
Inadequate or inappropriate access controls;
Deceit; and
Disasters at Chambers premises i.e. fire or flood.

If you are unsure whether a particular circumstance or incident constitutes a data protection breach, please refer the matter to the Data Protection Officer or another suitable person in their absence for guidance.

Reporting a personal data breach

All personal data breaches must be reported to the Data Protection Officer immediately upon discovery.

Reports should be made by e-mailing the Data Protection Officer.

Managing data protection breaches

There are four key steps to our data protection breach management plan:

Containment and recovery
Assessment and ongoing risk
Notification of breach
Evaluation and response

Containment and recovery

The Data Protection Officer, in conjunction with the reporting person, must:

Take steps to recover any lost data and limit the damage that the breach can cause where possible;
Decide who will lead the investigation into the breach; and
Find out who needs to be aware of the breach and tell those persons what they are expected to do (if anything) to assist in the containment and recovery of the breach.

Assess the risks

The Data Protection Officer must assess the potential adverse consequences of the breach for the individuals concerned (the people that the personal data in question belongs to), the potential severity or scale of the breach and the likelihood of the adverse consequences occurring.

Notification of breaches

The Chambers has a duty to report all data protection breaches that are likely to result in a risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO).

The Data Protection Officer is responsible for ensuring that all relevant data protection breaches are reported to the ICO without delay and no later than 72 hours after having become aware of it.

The Data Protection Officer will report the breach to the ICO in accordance with the reporting methods set by the ICO.

Where deemed appropriate, the individuals affected by the data protection breach, must also be informed. The Data Protection Officer must provide individuals with specific and clear information about what has happened and what is being done to address the breach. Advice should also be offered on any steps that the individual can take to protect themselves. The individuals must be given contact details should they require further information or help.

Considerations must also be made as to whether any other third parties should be notified i.e. the Police, insurers, professional bodies, the bank etc.

Evaluation and response

The final step is to evaluate the Chambers' response to the data protection breach.

It is important to establish whether the breach was caused by an isolated incident or is part of a wider systematic issue so that we can try to stop the same or a similar breach from occurring in the future.

Any lessons learned should be shared across the Chambers as appropriate.

The Data Protection Officer will review all any records of data breaches periodically to establish any trends requiring further attention.

Recording a data protection breach

There must be a central record of all data protection breaches that occur. The Data Protection Officer is responsible for maintaining a data protection breach register.