DATA PROTECTION POLICY

(includes General Data Protection Regulations)

DATA PROTECTION LAW

This Data Protection Policy ensures Rapleys LLP and all subsidiaries thereof:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.
- Complies with the General Data Protection Regulations.

The Data Protection Act 1998 describes how organisations – including Rapleys LLP and all subsidiaries – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by the principles below. These say that personal data must:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.

Rapleys LLP and all subsidiaries are registered with the Information Commissioner's Officer under reference number Z5975225.

PEOPLE, RISKS AND RESPONSBILITES

Policy Scope

This policy applies to:

- The head office of Rapleys LLP and all subsidiaries.
- All branches of Rapleys LLP and all subsidiaries.
- All staff and volunteers of Rapleys LLP and all subsidiaries.
- All contractors, suppliers and other people working on behalf of Rapleys LLP and all subsidiaries.

It applies to all data that the company holds relating to identifiable individuals or property information and accounts information, even if that information technically falls outside of the Data Protection Act 1998.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Account information

...plus any other information relating to individuals

Data Protection Risks
This policy helps to protect Rapleys LLP and all subsidiaries from some very real data security risks, including:

- Breaches of confidentiality.
- Failing to offer choice.
- Reputational damage.

Responsibilities
Everyone who works for or with Rapleys LLP and all subsidiaries has some responsibility for ensuring data is collected, store and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

Equity Partners
Ultimately responsible for ensuring that Rapleys LLP and all subsidiaries meet their legal obligations.

QHSE Compliance Team
- Responsible for keeping the partnership up to date on responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging for training and advice for all covered by this policy.
- Handle data protection queries from staff and anyone else covered this policy.
- Checking and approving any contracts or agreement with third parties that may handle the company's sensitive data.

It Manager:
- Ensuring all systems, services and equipment used for storing data meeting acceptable security standards.
- Perform regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluate any third party services the company is considering using to store or process data.

Marketing Manager:
Responsible for all statements attached to communications particularly with journalists or media outlets like newspapers and to ensure marketing initiatives abide by data protection principles.

Data Controllers
Responsible for all uploading of information, updating of information and access controls to information.

Key Individuals Within Rapleys:

Equity Partnership Representative:	Scott Hopper
QHSE Representative:	Helen Earwaker
IT Manager:	Scott Hopper
Data Controller:	Claire Hutchcraft
Data Controller:	Karen Wilcox

GENERAL STAFF GUIDELINES

The only people able to access data covered by this policy should be those who need to for their work. Data should not be shared informally.

Rapleys LLP and all subsidiaries will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people either within the company or externally.
- Data should be regularly reviews and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their Head of Department or the GDPR Team if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data Controller.

When data is stored on paper, it should be kept in a secure placed where people unauthorised cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved computing service.
- Servers containing personal data should be stored in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard back up procedures.

All mobile devices such as tablets or smart phones must be pin protected and username/passwords in place. All servers and computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to Rapleys LLP and all subsidiaries unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers.

DATA ACCURACY

The law requires Rapleys LLP and all subsidiaries to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- Rapleys LLP and all subsidiaries will make it easy for data subjects to update information Rapleys LLP and all subsidiaries holds about them.
- Data should be updated as inaccuracies are discovered.

DISCLOSING DATA

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies, without the consent of the data subject.

Under these circumstances, Rapleys LLP and all subsidiaries will disclose requested data. However, the GDPR Team will ensure the request is legitimate, seeking assistance form the Partnership and the company's legal advisers where necessary.

SPECIFIC RAPLEYS REQUIREMENTS

Majority of data is in electronic format. Any data on paper is placed in a file and stored in located in locked cabinets. Servers are stored in our Huntingdon site.

- Users are required to enter a secure username and password combination before gaining access to any data.
- User passwords must meet complexity requirements and must be changed every 30 days.
- Data is securely stored on designated drives and servers with restricted file and folder access where appropriate.
- Data is backed up at least once per day and a copy is held off site.
- Servers and computers have appropriate firewalls and virus checking software in place.
- All screens are locked when left unattended.
- All staff access is removed as soon as personnel leave Rapleys employment.
- Rapleys have a current and operational IT Disaster Recovery policy in place alongside a Business Continuity Plan.

COMPLIANCE CONFIRMATION

Please take the time to read the new Data Protection Policy and if you have any queries or concerns, please contact Scott Hopper or Helen Earwaker.

Please confirm that you have read and understood the Data Protection Policy by signing and returning at your earliest opportunity. A copy of this will be retained on your personnel file.

I confirm I have read and understood the Data Protection Policy.

Name:	
Date:	
Signed:	