	QAP 194 **REVISION AA1** **JANUARY 2019**

DATA PROTECTION POLICY

Context and overview

Key details

Policy prepared by:	Knight Group
Approved by board / management on:	Knight Group
Policy became operational on:	25/05/2018
Next review date:	25/05/2020

Introduction

Knight Group needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Knight Group:

* 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

Data protection law

The Data Protection Act 1998 describes how organisations — including Knight Group 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 eight important principles. These say that personal data must:

1. Be processed fairly and lawfully

2. Be obtained only for specific, lawful purposes

3. Be adequate, relevant and not excessive

4. Be accurate and kept up to date

5. Not be held for any longer than necessary

6. Processed in accordance with the rights of data subjects

7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

- Policy scope
- This policy applies to:
- The head office of Knight Group
- All sites of Knight Group
- All staff of Knight Group

All contractors, suppliers and other people working on behalf of Knight Group

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Data protection risks

This policy helps to protect Knight Group from some very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately.

Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Knight Group has some responsibility for ensuring data is collected, stored and handled appropriately.

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

The Company must:

- Manage and process personal data properly
- Protect the individuals' right to privacy
- Provide an individual with access to all personal data held on them.

The Company has a legal responsibility to comply with the Act. The Company, as a corporate body, is named as the Knight Group under the Act.

Knight Groups are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The Company is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website.

Information has to comply with the Act when managing that information.

The Company is committed to maintaining the eight principles at all times. This means that the Company will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.

- check the quality and accuracy of the information held

- apply the records management policies and procedures to ensure that information is not held longer than is necessary

- ensure that when information is authorised for disposal it is done appropriately

- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- only share personal information with others when it is necessary and legally appropriate to do so

- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act.

- train all staff so that they are aware of their responsibilities and of the Companies relevant policies and procedures.

General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

Knight Group 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 reviewed 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 line manager 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 your line manager.

When data is stored on paper, it should be kept in a secure place where unauthorised people 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, like on a printer.

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 USB, 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 cloud computing services.

Servers containing personal data should be sited 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 backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

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 Knight Group 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. In particular, it should never be sent by email unless secured or encrypted.

Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

Personal data should never be transferred outside of the European Economic Area.

Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Knight Group to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Knight Group should put into ensuring its accuracy.

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. For instance, by confirming a customer's details when they call.

Knight Group will make it easy for data subjects to update the information Knight Group holds about them.

Data should be updated as inaccuracies are discovered.

Subject access requests

All individuals who are the subject of personal data held by Knight Group are entitled to:

Ask what information the company holds about them and why.

Ask how to gain access to it.

Be informed how to keep it up to date.

Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Knight Group at mail@knightgroup.co.uk The Knight Group can supply a standard request form, although individuals do not have to use this.

The Knight Group will aim to provide the relevant data within 14 days.

The Knight Group will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

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, Knight Group will disclose requested data. However, the Knight Group will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Knight Group aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used

* How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.