# General

Data protection rules exist to protect the rights of living individuals when information about them is collected and used.

This policy is intended to help:

### complying with data protection law

### protect the rights of staff, workers, contractors, clients, customers and others

### minimise the risks of a data breach.

Personal information (that is information about living individuals) must be collected and dealt with appropriately, whether it is on paper, on a computer, or in the cloud or any other device (including smartphones).

We decide what personal information will be held, how, and what it will be used for. We are the “data controller” under the Data Protection Act.

We will register with the Information Commissioner unless we are exempt.

### You should keep yourself up to date with data protection requirements as they change and make sure that you properly handle our data and client data in accordance with those requirements.

### Request help from us if you are unsure about any aspect of data protection.

# Data principles

Everyone must abide by the eight “data protection principles”. They are set out and explained here:

<https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>

In summary, the Principles require that personal information is:

1. processed fairly and lawfully, and only if specific conditions are met;
2. obtained only for, and processed compatibly with, lawful specified purposes;
3. adequate, relevant and not excessive in relation to those purposes;
4. accurate and, where necessary, kept up to date;
5. not be kept for longer than is necessary;
6. processed in accordance with the rights of data subjects;
7. protected in appropriate ways;
8. not transferred outside the European Economic Area unless that country or territory also ensures adequate levels of protection.

# Responsibilities

Everyone accessing or handling our data is responsible for ensuring data is collected, stored and handled appropriately in line with this policy and the data protection principles. If you think our data handling processes breach a data protection principle, raise it with your Manager in writing, giving reasons.

# Obligations

## General

### You should only have access to personal data that you need for your work, and you should only use it for authorised activities.

### If you need access to confidential or personal information that you do not have, ask us. Tell us if you appear to have access to more data than you need.

### Review data regularly and report if it is out of date.

### Do not disclose personal data to anyone unless you have been directly told to do so and then only do so on that specific occasion in the way you have been asked to unless it is absolutely clear this is a general (repeating) instruction.

## Data storage

When personal 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, keep paper or files in a **locked** drawer or filing cabinet.

### 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:

### Use strong passwords (letters, numbers and symbols). Change them regularly, and do not share them except when you are required to disclose them to us.

### Where data is stored on removable media (like a data stick, USB, CD or DVD), password protect or encrypt the data. Keep the media securely locked away when not in use.

### Only store data on designated drives and servers. Only upload it to cloud computing services approved by us.

### Encrypt and password protect your backups. Back up data frequently, and test backups regularly.

### Personal data should not be saved directly to laptops or other mobile devices like tablets or smart phones unless you are specifically authorised to save to that device.

### All servers and computers and devices containing personal data should be protected by approved security software and a firewall, encrypted and behind strong password protection.

## Data use

The greatest risk of loss, corruption or theft of personal data is when you are accessing or using it.

### Lock the screen of your computer when unattended.

### Never send personal data by open email, as this is not secure.

### Encrypt and/or password protect data before transferring it electronically.

### Only share data with authorised contacts.

### Do not transfer personal data outside the European Economic Area without our specific consent.

### Do not save copies of personal data to any computer other than the one authorised by us.

## Data accuracy

We are all responsible for keeping personal data accurate and up to date.

### Do not create any copies of data or start collecting additional data we have not asked you to.

### Data should be updated as inaccuracies are discovered. For instance, if a person can no longer be reached on their stored telephone number, it should be removed from the database.

## Subject access requests

If anyone contacts you requesting information we hold about them, refer the matter immediately to us.