Phoenix Learning & Care Ltd
First Floor, Rolle Quay House, Rolle Quay, Barnstaple, Devon, EX31 1JE

Policy Number: 528
Data Protection

Introduction

Phoenix Learning and Care need to gather and use certain information about individuals.

The information can include; Customers, Suppliers, business contacts, employees and the vulnerable individuals and students we support.

This policy describes how personal data should be collected, handled and stored to meet the Company's data protection standards to ensure we comply with the law.

Why this Policy Exists

The data protection policy ensures we;

- Comply with data protection law and follow good practice
- Protect the rights of those individuals we support and ensure their privacy is protected
- Protect the rights of our Employees, Customers and business partners
- Provides transparency on our data protection principles and ethos
- Protects us from the risk of a data breach

Data Commissioner Registration Reference/s

The Phoenix Learning and Care organisation is registered with the Data Commissioner under the Data Protection Act 1998 and all storage and processing of personal data held in manual records or electronic storage mediums across the organisation and in each service should comply with the regulations of the Act.

Registration numbers;

Phoenix Childcare Ltd	Z2071709
Phoenix Learning and Care Ltd	Z2071712

Other Phoenix Policies

Group Policy 504 Document and Records Archiving
Group Policy 545 Records, Record Keeping and Passing on Information
Group Policy 556 Acceptable Use (Information Technology)
Group Policy 557 Bring Your Own Device
Group Policy 565 Data Breach

The Data Protection Law

The Data Protection Act 1998 describes how organisations like ours should collect, handle and store personal information irrespective of the medium (i.e. paper, electronic or other). 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 be;

- obtained and used fairly and lawfully
- used for limited and specifically stated purpose
- adequate, relevant and not excessive
- kept accurate and up to date
- not kept for longer than is necessary
- handled according to people's data protection rights and kept safe and secure
- not transferred outside the European Economic Area (EEA) without adequate data protection

Scope and Responsibilities

This Policy applies to all employees, volunteers, contractors and suppliers and other people working on behalf of the Phoenix Learning and Care.

It applies to ALL data that the company holds relating to identifiable individuals, even if this information technically falls outside of the Data Protection Act 1998. This can include;

- Name of individuals
- Postal addresses
- Email Addresses
- Telephone numbers
- Personal medical information
- Gender type
- Plus any other information relating to individuals

Data Protection Risks

This policy helps protect Phoenix Learning and Care from some very real data security risks, including;

- **Breaches of Confidentiality** – For instance, information being given out inappropriately
- **Failing to Offer Choice** – For instance, individuals should be free to choose how the company uses data relating to them
- **Reputational Damage** – For instance, the company could suffer if unapproved access to sensitive data was allowed.

Data Controller

The *Data Controller* for the organisation is the Group Finance Manager. This role reports directly to the Phoenix board in terms of Data Protection.

Data Protection Audit and Registers

The company has completed a Data Protection Audit to identify what personal information is held and what it does with this information. This audit is periodically updated. A register of Data processing activity is available.

Consent

In order to process personal information and to meet legislative requirements consent has to be freely given, specific, informed and unambiguous. Consent must also be a positive indication of agreement and it cannot be inferred from silence, pre-ticked boxes or inactivity. In relation to Children the processing of data related to Children under 16 requires the person with parental responsibility to give consent.

Statements facilitating consent are added to specific documents as required.

General Employee Guidelines

The following principles apply;

- 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.
- Phoenix Learning and Care will provide training opportunities for employees in *report writing* and *professional boundaries*.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below;
    - 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 delete and disposed of. (Please refer to Group Policy 504 Documents and Records Archiving)
    - Employees **should request help** from their line manager or the Data Protection Officer 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 Team or Data Controller.

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;

- When not required the paper or files should be kept in a a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where any unauthorised people can see them. This includes leaving documents on, or near, 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. Always use the passwords provided to access the Phoenix computer systems and not abuse them by passing them on to people who should not have them and ensure passwords are changed accordingly as required. Ensure good password management by ensuring passwords are not easily 'guessed'.
- Use computer screen security blanking where appropriate to ensure that personal data is not openly visible.
- If data is stored on removable media (like a CD or DVD) these should be kept locked away securely when not in use.
- Data should only be stored on designated drives and servers and should only be uploaded using approved cloud devices.
- Servers containing personal data should be sited in a secure location away from general office space.
- Data should be backed up frequently. These back-ups should be tested regularly in-line with the company's standard back-up procedures.
- Data should never be saved to laptops of 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 stored electronically should be filed on Company supplied specific recording databases which have suitably secure data back-up and archiving (i.e. ADP/BWC).
- Microsoft Office data (i.e. word, power point, excel) should be stored on service specific drive locations (e.g. H drive) that is only accessible to appropriate employees. Under no circumstances should sensitive data be stored on local computer machine hard-drives, memory sticks or drives accessible to wider members of staff (i.e. u drive).

Data Use

Personal data is of no value to Phoenix Learning and Care unless the organisation can make use of it. However it is of value 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 screens of their computers are always locked when unattended.
- Personal data should not be stored informally, In particular it should never be sent by email, this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT team can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the EEA.
- Employees should never save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy and the Right to Rectification

The law requires Phoenix Learning and Care to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that personal data is accurate, the greater effort Phoenix will 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 accurate and up-to-date as possible by ensuring;

- Data will be held in as few places as necessary. Employees should not create any unnecessary data sets.
- Employees should take every opportunity to ensure data is updated.
- Phoenix will endeavour to make it easy for data subjects (i.e. individuals) to update information the company holds about them.
- Data should be updated without any “undue delay” as data inaccuracies are discovered.
- Individuals should be notified when the rectification has been carried out.

Right to Erasure (also known as the “right to be forgotten”)

An individual has the right to data erasure of personal information where the;

- personal information is no longer necessary for the purpose to which it was collected or otherwise processed.
- individual withdraws consent for the processing (if processing was based on consent).
- individual objects to the processing which is based on legitimate interests grounds or use for direct marketing.
- process is unlawful
- personal information needs to be erased in order to comply with a legal obligation

The individual should be notified when the erasure has been carried out.

Archive/Destruction of Data

Please refer to Group Policy 504 Documents and Records Archiving

Right to Restrict Processing

An individual can require Phoenix to restrict processing if;

- The accuracy of the personal information is contested by the individual
- The processing is unlawful but the individual does not want the personal information erased.
- The organisation no longer needs the personal information for the purposes of processing but it is required by the individual for the establishment, exercise or defence of legal claims
- The individual has objected to the processing pending verification whether the organisation has legitimate grounds to override those of the individual.

Right to Data Portability

The right to data portability aims to make it easier for individuals to change service providers and the transfer of applicable information to the new provider. Phoenix will support this process as required.

Right to Prevent Automated Decision Making and Profiling

An individual has the right to prevent an organisation from using automated decision making or profiling that decision making procedure produces legal effects concerning the individual. Automated decision making is by nature rare within our operations but Phoenix will comply with reviewing any instances of this.

Data Protection Impact Assessments

It is legal obligation to carry out a *Data Protection Impact Assessment* when new products or services are developed where the processing of data is likely to result in a high risk to the rights and freedoms of an individual. Phoenix will undertake this as applicable.

Subject Access Request/s (SAR)

The organisation believes that access to information and security and privacy of data is an absolute right of every employee or individual we support and that these groups are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

All individuals who are the subject of personal data held by the company 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* (SAR).

SAR's **MUST** be made in writing (ideally) to the Data Controller.

The Data Controller will **ALWAYS** identify the identity of anyone making a SAR **BEFORE** handing over any information.

Where an individual we support wishes to see any information held about them, this should be actively facilitated and appropriate advice and support given. This may include the involvement of an advocate.

The Data Protection Act gives an individual several rights in relation to the information held about them. Of particular relevance in a health and social care setting, is the right of individuals to seek access to their records held by the health or social care provider.

Access covers the right to obtain a copy of the record in permanent form, unless the supply of a copy would involve disproportionate effort or the individual agrees that his/her access rights can be met some other way, for example, by viewing the record.

A response to A SAR will be given promptly and in any event within **1 month** of the request. If the application does not include sufficient details to identify the person making the request or to locate the information, those details should be sought promptly and the 40-day period begins when the applicable details have been supplied.

No charge will be made for a Subject Access Request.

The individual will receive the following information;

- The purposes of the processing
- The categories of personal information
- Any third parties who have received or may have received the information
- If any international third parties having received the information, the safeguards in place to protect the personal information
- How long that the personal information will be stored and what criteria is used to work out that period (typically legislative).

- Existence of the right to request rectification, erasure, restriction or to object to processing
- The right to complain to the ICO
- If an individual did not give the information to the organisation, where did it come from
- Whether there is an automated decision making and some meaningful information about the logic involved as well as the significance and envisaged consequences on the individual.

Once access to the data has been given, there is no obligation to give access again until a reasonable period has elapsed. What is reasonable depends on the nature of the data, the purposes for which it is processed and the frequency with which it has been altered.

There are two main exemptions from the requirement to provide access to personal data in response to a subject access request. These are:

- If the record contains third-party information (e.g. not about the patient or the treating clinician) where that third party is not a healthcare professional and has not consented to their information being disclosed. If possible, the individual should be provided with access to the part of the record that does not contain the third-party identifier.
- If access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible, the individual should be provided with access to that part of the record that does not pose the risk of serious harm.

Data Breach

Any data security breach must be reported to the ICO within 72 hours of becoming aware of fit unless the breach is unlikely to result in risk to the rights and freedoms of individuals.

Group Policy 565 Data Breach defines the process to be followed in the case of a data breach being discovered.

Communication and Training

All new employees are made aware of the Company Policies and Procedures as part of their induction. Policies and procedures are also signposted as part of the Employee handbook. Employees spend time discussing data privacy, confidentiality and protection as part of the induction.

Existing employees can request training covering basic information about confidentiality, data protection and access to records from their line manager.

All Colleagues who need to use the computer system should be appropriately trained and coached in its use.

All policies are available on the 'U' drive which all employees can access and are reviewed annually.

Providing Information

Phoenix Learning and Care aims to ensure that individuals are aware that their data is being process and that they understand;

- How the data is being used
- How to exercise their rights

To support this, the company has a privacy statement, setting out how data relating to individuals is used by the Company. This is available via our website/s.