Data Protection

POLICY STATEMENT

- 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.

Document Control			
Policy Code:	GRP 528	Policy Owner:	Data Protection Officer
Version:	21.05_v1.05	Policy Author(s):	François Delbaere (Data Protection Officer)
Date ratified:			
Review Frequency:	3 years		
Next review date:	May 2024	Ratifying Committee:	EMT

Document History (last 3 versions)			
Date of Issue	Version No.	Person(s) responsible for change	Nature of Change
21/05/2021	1.05	François Delbaere	Inclusion of information on vehicle management system.

CONTENTS

1. Introduction

1.1 Why this Policy Exists

1.1.1 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

1.2 Data Commissioner Registration Reference(s)

1.2.1 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.

1.2.2 Registration numbers:

- Phoenix Childcare Ltd: Z2071709
- Phoenix Learning and Care Ltd: Z2071712

1.2.3 Other Phoenix Policies

- Group Policy 504 Document and Records Archiving
- Group Policy 545 Records, Record Keeping and Passing on Information
- Group Policy 533 Company Vehicles (inc Driving at Work)
- Group Policy 556 Acceptable Use (Information Technology)
- Group Policy 557 Bring Your Own Device
- Group Policy 565 Data Breach

1.3 The Data Protection Law

1.3.1 The Data Protection Act 1998 and The General Data Protection Regulation 2016/679 (a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area which also addresses the export of personal data outside the EU and EEA areas) 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.

1.3.2 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

1.4 Scope and Responsibilities

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

1.4.2 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

2. Data Protection

2.1 Data Risks

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

2.1.2 Breaches of Confidentiality – For instance, information being given out inappropriately

2.1.3 Failing to Offer Choice – For instance, individuals should be free to choose how the company uses data relating to them

2.1.4 Reputational Damage – For instance, the company could suffer if unapproved access to sensitive data was allowed.

2.2 Data Controller

2.2.1 The *Data Controller* for the organisation is the Group Finance Director. This role reports directly to the Phoenix board for matters of Data Protection.

2.3 Data Protection Audit and Registers

2.3.1 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.

2.4 Consent

2.4.1 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.

2.4.2 Statements facilitating consent are added to specific documents as required.

2.5 General Employee Guidelines

2.5.1 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.

2.6 Data Storage

2.6.1 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.

2.6.2 When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

2.6.3 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

2.6.4 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).
- 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).

2.7 Data Use

2.7.1 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 European Economic Area (EEA).
- Employees should never save copies of personal data to their own computers. Always access and update the central copy of any data.

2.8 Data Accuracy and the Right to Rectification

2.8.1 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.

2.8.2 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.

2.9 Right to Erasure (also known as the "right to be forgotten")

2.9.1 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 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

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

2.10 Archive/Destruction of Data

2.10.1 Please refer to Group Policy 504 Documents and Records Archiving

2.11 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.

2.12 Right to Data Portability

2.12.1 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.

2.13 Right to Prevent Automated Decision Making and Profiling

2.13.1 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.

2.14 Data Protection Impact Assessments

2.14.1 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.

2.15 Subject Access Request(s) (SAR)

2.15.1 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.

2.15.2 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

2.15.3 If an individual contacts the company requesting this information, this is called a *Subject Access Request* (SAR).

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

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

2.15.6 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.

2.15.7 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.

2.15.8 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.

2.15.9 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.

2.15.10 No charge will be made for a Subject Access Request.

2.15.11 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.

2.15.12 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.

2.15.13 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.

2.16 Data Breach

2.16.1 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.

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

2.17 Communication and Training

2.17.1 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.

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

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

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

2.18 Providing Information

2.18.1 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

2.18.2 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 and shown as an Appendix to this Policy

3. Appendix A - Protecting your Privacy

3.1 Introduction

3.1.1 This Privacy Notice explains the types of personal data we may collect about individuals when they interact with Phoenix. It also explains the organisational approach to the handling and storage of data and to keep it safe. It is important that as a company Phoenix develops and maintains the trust and confidence of its customers, employees, contractors, and critically the individuals we support to respect data and handle it with the right ethos.

3.1.2 The purpose of this statement is to inform individuals about their rights, and how the Phoenix Group of companies uses the data appertaining to individuals.

3.1.3 The following sections should answer many questions you have but if not, please do get in touch with us.

3.1.4 This Privacy Notice will be updated from time to time.

3.2 What is Phoenix Learning and Care?

3.2.1 The Phoenix Group of Companies – which we'll refer to as 'Phoenix' in this document – is made up of a number of component companies:

- Phoenix Learning and Care Holdings Ltd (Reg 07899184)
- Phoenix Childcare Ltd (Reg 05506172)
- Phoenix Learning and Care Ltd (Reg 03586226)
- Phoenix Learning and Care Property Ltd (Reg 09872260)

3.2.2 For simplicity throughout this notice data appertains to the following groups of people (including, prospect, current and past):

- Individuals Phoenix support
- Customers
- Employees
- Volunteers
- Contractors

3.3 Explaining the legal bases Phoenix rely on

3.3.1 The law on data protection sets out a number of different reasons for which a company may collect and process an individual's personal data, including:

- Consent - In specific situations, the collection and processing of an individual's data with their consent.
- Contractual obligations - In certain circumstances, the need to acquire personal data to comply with an organisation's contractual obligations.

- Legal compliance - If the law requires an organisation, it may need to collect and process an individual's data.

- Legitimate interest - In specific situations, an organisation may require an individual's data to pursue its legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests.

3.4 When do Phoenix collect personal data?

3.4.1 When an individual applies for a job vacancy with the Company.

3.4.2 When an individual becomes an employee through their employment with the Company.

3.4.3 When the Company provides a service to an individual we support.

3.4.4 When an individual contacts the Company by any means with an enquiry.

3.4.5 When an individual has given a third-party permission to share with Phoenix the information Phoenix hold about that individual.

3.5 What sort of personal data does Phoenix collect?

3.5.1 Data related to job vacancy applications (e.g. name, address, career history, qualifications and experience).

3.5.2 Data relating to employment (supervisions, appraisals, records of meetings/activity, employee relations, health conditions that affect duties and responsibilities, remuneration).

3.5.3 Information for individuals the Company supports (e.g. health and social care data, history and individual preferences).

3.5.4 Images may be recorded on CCTV when people visit certain locations in the company's portfolio of services.

3.5.5 Individual's contact details, if they interact with Phoenix through appropriate channels, to help Phoenix respond to the individual's comments, questions or feedback.

3.6 How and why do Phoenix use personal data?

3.6.1 Phoenix strive to provide the best possible standard of care so that the individuals supported are valued equally, listened to and included. One way to achieve that is to get the richest picture the company can of the individual by combining the data we have about an individual. The data privacy law allows this as part of a legitimate interest in understanding those Phoenix support and providing the highest levels of service to them. The information Phoenix collect is used for purpose of establishing and planning what care provision is needed, where and when, including preparation for health emergencies.

3.6.2 In order to provide the care described above Phoenix need to employ the most appropriate individuals with the right skills, values and attitudes. Tri-angulating a job applicant's career history, character and experience helps Phoenix recruit the right employees robustly using safer recruitment principles.

3.6.3 Here's how Phoenix use personal data and why:

- To protect the business and individuals from fraud and other illegal activities. If Phoenix discover any criminal activity or alleged criminal activity through its policies and procedures it will process this data for the purposes of preventing or detecting unlawful acts.
- To safeguard and protect the individuals Phoenix support and provide the best possible level of care and support the company can to that individual.
- To send communications required by law or which are necessary to inform individuals about any changes to the service/s Phoenix provide. These communications will not include any promotional content and do not require prior consent. If Phoenix do not use personal data for these purposes, it would be unable to comply with the legal obligations or be able to provide a service to the individual concerned.
- To comply with Phoenix's contractual and/or legal obligations to share data with law enforcement (e.g. when a court order is submitted to share data with law enforcement agencies or a court of law).
- To send survey and feedback requests to help improve Phoenix's services. These messages will not include any promotional content.

3.6.4 Phoenix does not use any individual's data for direct or indirect marketing purposes of any type.

3.6.5 Phoenix does not sell or trade any individual's data to any other organisation.

3.7 How Phoenix protect individual's personal data

3.7.1 Phoenix know how much data security matters to all prospective and actual employees and the individuals it supports. Phoenix will treat an individual's data with the utmost care and take all appropriate steps to protect it.

3.7.2 Phoenix achieves this by having policies appertaining to the recording, storing and processing of information. Phoenix provides its employees training in handling data appropriately including: professional boundaries, record keeping and data protection.

3.7.3 Information systems are encrypted and IT storage facilities are secure. Documents are kept securely locked.

3.7.4 Phoenix has arrangements for the disposal of confidential records.

3.8 How long will Phoenix keep personal data?

3.8.1 Whenever Phoenix collects or processes an individual's personal data, we'll only keep it for as long as is necessary for the purpose for which it was collected or indeed a period as laid down by statute.

3.8.2 At the end of that retention period, data will either be deleted completely or anonymised, for example by aggregation with other data so that it can be used in a non-identifiable way for statistical analysis and business planning.

3.9 Who do Phoenix share an individual's personal data with?

3.9.1 Phoenix sometimes will share an individual's personal data with trusted third parties.

3.9.2 Phoenix provide only the information those parties need to perform their specific service(s).

3.9.3 They may only use an individual's data for the exact purposes Phoenix specify in its contract/s with those third parties.

3.9.4 Phoenix work closely with suppliers to ensure that an individual's privacy is respected and protected at all times.

3.9.5 If Phoenix stop using a supplier's services Phoenix will ensure that an individual's data held by them will either be deleted, rendered anonymous or supplied to us.

3.9.6 Examples of the kind of third parties Phoenix work with are IT companies who support Phoenix's website and other business systems (e.g. payroll, care/incident management).

3.9.7 For fraud management, Phoenix may share information about fraudulent or potentially fraudulent activity in its premises or systems. This may include sharing data about individuals with law enforcement bodies.

3.9.8 Phoenix may also be required to disclose personal data to the police or other enforcement, regulatory or Government body, upon a valid request to do so. These requests are assessed on a case-by-case basis and take the privacy of individuals into consideration.

3.10 Where personal data may be processed

3.10.1 Phoenix do not share personal data with third parties outside the European Economic Area (EEA).

3.10.2 Any transfer of an individual's personal data will follow applicable laws and Phoenix will treat the information under the guiding principles of this Privacy Notice.

3.11 What are an individual's rights over their personal data?

3.11.1 Remember, if an individual chooses not to share their personal data with Phoenix, or refuse certain contact permissions, Phoenix might not be able to provide support to or indeed employ an individual.

3.11.2 An individual has the right to request:

- Access to the personal data Phoenix hold about them, free of charge in most cases.
- The correction of personal data when incorrect, out of date or incomplete.
- That Phoenix stop using their personal data for direct marketing (either through specific channels, or all channels).
- That Phoenix stop any consent-based processing of their personal data after they withdraw that consent.

- Review (by a Phoenix employee) of any decision made based solely on automatic processing of the individual's data (i.e. where no human has reviewed the outcome and criteria for the decision).

3.11.3 The applicable individual can contact Phoenix to request to exercise these rights at any time.

3.11.4 If Phoenix choose not to action the request Phoenix will explain the reasons for refusal.

3.11.5 The individual's right to withdraw consent:

- Whenever an individual has given Phoenix their consent to use their personal data, they have the right to change their mind at any time and withdraw that consent.

3.11.6 Where Phoenix rely on our legitimate interest:

- In cases where Phoenix are processing an individual's personal data on the basis of our legitimate interest, an individual can ask Phoenix to stop for reasons connected to their individual situation. Phoenix must then do so unless we believe Phoenix have a legitimate overriding reason to continue processing the individual's personal data.

3.11.7 Checking an individual's identity:

- To protect the confidentiality of an individual's information, Phoenix will ask them to verify their identity before proceeding with any request they make under this Privacy Notice.

3.11.8 If the individual has authorised a third party to submit a request on their behalf, Phoenix will ask them to prove they have the individual's permission to act.

3.12 Contacting the Regulator

3.12.1 If an individual feels that their data has not been handled correctly, or they are unhappy with Phoenix's response to any requests they have made to Phoenix regarding the use of their personal data, they have the right to lodge a complaint with the Information Commissioner's Office.

3.12.2 The information Commissioners Office can be contacted by calling 0303 123 1113 or visit www.ico.org.uk

3.12.3 Phoenix is registered with the Information Commissioner's Office.

3.13 Any questions?

3.13.1 Phoenix hope this Privacy Notice has been helpful in setting out the way it handles individual's personal data and the individual's rights to control it.

3.13.2 If you have any questions that haven't been covered, please contact our Data Protection Officer who will be pleased to help you:

3.13.3 Email us at dpo@plcl.org.uk with the words *For the attention of the Data Protection Officer* in the title bar.

3.13.4 Or write to us at:

Attn: Data Protection Officer
Phoenix Learning and Care
Unit 5 Chinon Court,
Lower Moor Way
Tiverton
Devon
EX16 6SS

4. Appendix B - Vehicle Maintenance System and data implications

4.1 Introduction and data protection principles

4.1.1 Phoenix Child Care Limited/Phoenix Learning and Care Limited (referred to collectively as the "Company" in this Vehicle Maintenance System Privacy Policy) are committed to protecting and respecting your personal data and privacy.

4.1.2 The Company has decided to adopt a vehicle maintenance system called Verizon Connect (the "System") in order to monitor the use of Company vehicles to provide greater oversight of their use and condition. The System will also allow the Company to monitor driver behaviour with an aim to promote increased awareness of health and safety requirements whilst driving.

4.1.3 The purpose of this Vehicle Maintenance System Privacy Policy ("Policy") is to inform employees and contractors ("you") about the use of the System, the reasons for its use and how the Company will use and collect personal data from you when:

- you use a Company vehicle which is connected to the System: and/or
- you access and use the System on Company computers and personal mobile phones

4.1.4 Whenever you provide personal data, we are legally obliged to use your information in line with all applicable laws concerning the protection of such information: including but not limited to the Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (UK GDPR), described in this policy as the "Data Protection Laws". We will comply with Data Protection Laws which state that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way:
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes:
- Relevant to the purposes we have told you about and limited only to those purposes:
- Accurate and kept up to date:
- Kept only as long as necessary for the purposes we have told you about: and
- Kept securely

4.1.5 This Policy does not form part of any employee's contract of employment or any contractors service contract and we may update this notice at any time but if we do so, we will provide you with an updated copy as soon as reasonably practical. This Policy should be read in conjunction with GRP 533 Company Vehicles.

4.2 What is the new vehicle maintenance system and why is it being used?

4.2.1 With the growth in our services across a wider geography it has become harder to centrally manage our fleet of Company vehicles which is increasing in size.

4.2.2 Previous manual checks and systems used by the Company did not provide live data and brought increased administrative burdens on our staff. The Company has therefore decided to adopt new technology by adopting the System to help manage the Company's fleet of vehicles.

4.2.3 We believe that such use is necessary for legitimate business purposes, including:

- to assist in the day-to-day management of Company vehicles including ensuring Company assets are used in the most efficient way whilst ensuring the health and safety of staff, people we support and others is protected:
- to help improve the driving behaviour of staff and contractors which will in turn reduce the number of incidents or potential near misses and act as a deterrent against crime and inappropriate driving behaviour:
- to ensure that all Company vehicles abide by all relevant legislation applicable whether it be speed limits, or regular vehicle servicing, repair and maintenance and enable the Company to take action where necessary:
- for the personal safety of staff and people we support as the System will provide management with live data about the location and status of Company vehicles and a GPS connection will allow drivers to use the System to send out an alarm to alert people of their need for assistance in the event of an emergency:
- to keep a record of driving routes, driving data and locations to support any possible internal or external investigations:
- to identify and evidence any repeated or specific issues that may need to be addressed through either disciplinary or capability procedures:
- to support law enforcement bodies in the detection and prosecution of crime:
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings:
- to assist in the defence of any civil litigation, including employment tribunal proceedings or third-party liability disputes (and thus potentially reduce insurance claims and premiums): and
- to foster and maintain a culture of regular inspections, management and care for Company vehicles through reviewing information collated and managing needs:
- This list is not exhaustive and other purposes may be or become relevant.

4.2.4 We have carefully considered if the use of the System is appropriate by carrying out a privacy impact assessment (PIA) and an accompanying legitimate interests assessment (LIA). The PIA and LIA have assisted us in deciding whether the new System is necessary and proportionate in the circumstances and whether it should be used at all or whether any limitations should be placed on its use. The PIA and LIA have considered the nature of the problem that we are seeking to address at this time and whether the use of the System is likely to be an effective solution, or whether a better solution exists. In particular, they have considered the effect the System will have on individuals and therefore whether its use is a proportionate response to the problem identified. We have determined that the implementation of the System is proportionate.

4.2.5 Both the PIA and LIA can be made available on request.

4.2.6 It should be noted that this Policy does not apply to employees who currently have the use of company car benefit.

4.3 Personnel Responsible

4.3.1 The Data Protection Officer has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this Policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to managerial staff.

4.4 What personal data will be collected

4.4.1 The System will collect and process personal data about you. Typically, the personal data will include identity, contact, technical, profile and driving data such as:

- Identity Data includes first name, last name, title or other identifier (such as job title), signature.
- Contact Data includes email addresses and telephone numbers used for sending alerts through the System.
- Technical Data includes internet protocol (IP) address, your login data, time zone setting and location, and versions, operating system and platform, and other technology on the devices you use to access the System.
- Profile Data includes your username and password that you use to access the System.
- Driving Data includes information about vehicle status, driving activity and behaviour (speed etc), service locations and other GPS location information of the vehicle being driven which will be linked to the individual driving the vehicle by the use of a key fob.

4.4.2 Please note that other personal data may be collected and/or processed from time to time.

4.4.3 Special Categories of Personal Data about you will not be collected through use of the System and information about criminal convictions and offences will not be collected by the System.

4.5 How will your personal data be collected

4.5.1 Different methods will be used to collect data from and about you including through:

- Direct interactions. You may provide your Identity, Contact and Profile Data to us by providing it to us direct.
- Third parties. We will also receive personal data about you from Verizon Connect who is the third party provider of the System who will collect this personal data via the black boxes and key fobs in the Company vehicles and when you log into the System from a computer or mobile phone device.

4.6 How your data will be used

4.6.1 Information will be held about you to manage our fleet of Company vehicles. The System can provide both real time and historical journey, speed, and location information, as well as driver fob identification and this data will be stored in the System. Reports will be generated weekly and if certain thresholds are breached, a live alert will be sent to managers. Managers will also have the ability to view GPS live data online via the System, which will be used to help them manage resources and plan for arrivals/departures from a service. Managers' use of the System will be compartmentalised to the vehicle assets they are charged with monitoring.

4.6.2 We have set out below in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a user of the System	Identity Contact Profile	Necessary for our legitimate interests (to keep our records updated and ensure every employee can access and use the System)
To keep oversight of vehicle locations for the purposes of managing the Company vehicle fleet more effectively and for the personal safety of staff and people we support. To maintain a routine of regular inspections, management and care for Company vehicles through reviewing information collated and managing needs.	Driving Data Contact Profile	Necessary for our legitimate interests (to ensure the efficient use of the Company vehicle fleet, to ensure that all vehicles abide by all relevant legislation and take action where necessary, to locate employees in the event of an emergency by ensuring management know the exact location of any vehicle at any given time and enable the Company to monitor the safety of its lone workers). To comply with health and safety obligations.
To keep a record of driving routes, driving data and locations to support any possible internal or external investigations.	Driving Data Contact	Necessary for our legitimate interests (to ensure we comply with legal obligations and are able to investigate complaints adequately). To comply with health and safety obligations.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To administer and protect our business when using the System (including troubleshooting, data analysis, system maintenance and support).	Identity Contact Technical	Necessary for our legitimate interests (for ensuring the System is used correctly and is maintained).
To gather evidence for possible grievance or disciplinary hearings.	Identity Contact Technical Driving Data Profile	Necessary for our legitimate interests (to ensure inappropriate driving behaviour and associated health and safety concerns can be addressed). To comply with health and safety obligations.
To investigate and respond to complaints received by individuals in relation to misconduct, inappropriate behaviour or incidents resulting in damage to third party property, insurance claims or civil litigation.	Identity Contact Driving Data	Necessary for our legitimate interests (to manage claims and adequately deal with legal disputes involving you, or other employees, and contractors, people we support or other road users, to improve any insurance claims made and / or reduce the amount of third-party liability disputes).

4.7 Lawful basis for processing

4.7.1 We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

4.7.2 We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

4.8 Sharing data with third parties

4.8.1 Authorised managers will be given specific access to the System for operational maintenance and planning purposes. Their access will be compartmentalised to the vehicle assets they are charged with maintaining. Staff with access to the System will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

4.8.2 There may occasionally be times where the Company needs to share data with relevant authorities, for example if a safeguarding claim is raised and is then investigated by the police or any designated officers from the local authority. Such data will only be shared where it is lawful to do so.

4.8.3 In some circumstances the Company may also share data with insurance companies in the event that it is relevant to a claim.

4.9 Data security

4.9.1 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know it. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

4.9.2 We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

4.9.3 The third party (Verizon Connect) providing the System is engaged under a written contract with the Company with appropriate commitments to security included. The data is stored on Verizon Connect's data centres in the EU via a cloud application.

4.10 Equipment & System security

4.10.1 You are responsible for the security for any device used by you to access the System, whether it belongs to the Company or to yourself. You should lock your device or log off when leaving it unattended to prevent unauthorised users accessing the System in your absence. This Policy should be read in conjunction with GRP 557 Bring Your Own Device.

4.10.2 Passwords for the System must be kept confidential and changed regularly to ensure confidential data is protected.

4.11 Disciplinary action

4.11.1 Deliberate damage to the System, the key fobs or black boxes fitted to Company vehicles or attempts to change data in the System without permission shall be dealt with in accordance with the GRP 537 Disciplinary Policy.

4.11.2 Any employee found accessing, distributing, sharing or misusing any personal data collected via the System without lawful authority shall be dealt with in accordance with the GRP 537 Disciplinary Policy.

4.11.3 Where concerns are raised about an employee's working practice or driving behaviour, a manager may request information held in the System for consideration as part of the disciplinary investigation.

4.11.4 A breach of this Policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this Policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4.12 Data retention

4.12.1 We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation.

4.12.2 To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

4.12.3 In some circumstances you can ask us to delete your data (see below for further information).

4.12.4 We may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

4.13 SUBJECT ACCESS REQUESTS

4.13.1 Data subjects may make a request for disclosure of their personal information and this may include personal data collected by the System (data subject access request). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, which can be found in the GRP 528 Data Protection.

4.14 COMPLAINTS

4.14.1 If any member of staff has questions about this Policy or any concerns about our use of the System, then they should speak to their manager in the first instance.

4.14.2 Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.

4.14.3 People we support who have any concerns should be directed to the Data Protection Officer.

4.15 Requests to Prevent Processing

4.15.1 We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation 2016). For further information regarding this, please contact the Data Protection Officer on dpo@plcl.org.uk.