Internal Employee Data Protection Policy

In the course of your work you may come into contact with or use confidential information about employees, clients and customers, for example their names and home addresses. The **General Data Protection Regulations** (GDPR) contains principles affecting employees' and other personal records. Information protected by GDPR includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure that you do not breach the regulations. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from our Data Protection Officer, details of which can be found below.

You should be aware that, under GDPR, you are personally accountable for your actions and can be held criminally liable if you knowingly, or recklessly, breach it. Any serious breach of data protection regulations will also be regarded as misconduct and will be dealt with under the <insert dealership>'s disciplinary procedures. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal. The breach will also need to be reported to the regulator within 72 hours. Failure to do so will invoke fines, of which you may be personally liable.

In summary, under the GDPR, employees and data subjects have the following rights:

- The right to be informed, which encompasses the obligation on employers to provide transparency as to how personal data will be used.
- The right of access.
- The right to rectification of data that is inaccurate or incomplete.
- The right to be forgotten under certain circumstances.
- The right to block or suppress processing of personal data.
- The new right to data portability which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

<insert dealership> will only process your personal data as a contractual necessity (i.e. producing contracts of employment, paying our employees and appraisal purposes), and as a necessity for the compliance with a legal obligation (i.e. processing PAYE and NI information to HMRC), in the legitimate interests of the business and necessary processing for carrying out obligations under employment law. As such, please could you complete the form overleaf and return to HR/Payroll.

Employer Declaration

As a company, <insert dealership> have done the following:

- Put in place appropriate measures to ensure and demonstrate that we comply (this may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies).

- Conducted maintenance of relevant documentation on processing activities.

- Implemented measures that meet the principles of data protection by design and data protection by default (such as data minimisation, pseudonymisation, transparency, allowing individuals to monitor processing and creating and improving security features on an ongoing basis).

- Conducted data protection impact assessments where appropriate.

<insert dealership> will only use your personal data for HR and payroll administration. This administration includes processing monthly salaries, maintaining your personnel records and managing performance appraisals. If your contract of employment is terminated, we will hold your personnel data for seven years in line with HMRC guidelines, unless you exercise your right to be forgotten. We will not pass your data to any third parties without your consent.

*For further information on the General Data Protection Regulation (GDPR), please contact our HR and Payroll team or visit http://www.eugdpr.org/

The data protection principles

There are eight data protection principles that are central to GDPR. <insert dealership> and all its employees must comply with these principles at all times in its information-handling practices. In brief, the principles say that personal data must be the following:

1. Processed fairly and lawfully and must not be processed unless certain conditions in relation to personal data, and additional conditions are met in relation to sensitive personal data. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:
   - race or ethnic origin
   - political opinions and trade union membership
   - religious or other beliefs
   - physical or mental health or condition
   - sexual life
   - criminal offences, both committed and alleged

2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

3. Adequate, relevant and not excessive. <insert dealership> will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date

information and to check there is sound business reason requiring information to continue to be held.

4. Accurate and kept up-to-date. If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that <insert dealership>'s records can be updated. <insert dealership> cannot be held responsible for any errors unless you have given notification of the relevant changes.

5. Not kept for longer than is necessary. <insert dealership> will keep personnel files for no longer than seven years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which <insert dealership> decides it does not need to hold for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the GDPR.

7. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised employees. Data held on computer will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. <insert dealership> has network backup procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

Your personal information being held

<insert dealership> holds personal data about you. By signing the attached privacy notice, you understand that data will be processed by <insert dealership> for any purpose related to your continuing employment or its termination including, but not limited to, payroll, human resources and business continuity planning purposes. Agreement to <insert dealership> processing your personal data is a condition of your employment. This includes using your name, photograph and a brief work experience history in its marketing or promotional material, whether in hard copy print format or online on <insert dealership>'s website. It also includes supplying <insert dealership> with any personal data that it may request from you from time to time as necessary for the performance of your contract of

employment or the conduct of business, for example, supplying up-to-date contact telephone numbers to be held by line managers as part of its business continuity plan.

<insert dealership> also holds limited sensitive personal data about its employees and, by signing the attached privacy notice, you are aware of the holding and processing of that data, for example sickness absence records, health needs and equal opportunities monitoring data.

Your right to access personal information

You have the right, on request, to receive a copy of the personal information that <insert dealership> holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You also have the right on request to:

- be told by <insert dealership> whether and for what purpose personal data about you is being processed
- be given a description of the data and the recipients to whom it may be disclosed
- have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- be informed of the logic involved in computerised decision-making

Upon request, <insert dealership> will provide you with a statement regarding the personal data held about you. It will state all the types of personal data <insert dealership> holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request for this. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Data Protection Officer. GDPR states that you must receive the data you have requested within 30 days.
If you wish to make a complaint that these rules are not being followed in respect of personal data <insert dealership> holds about you, you should raise the matter with the Data Protection Officer.

If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under <insert dealership>'s grievance procedure.

Your obligations in relation to personal information

If, as part of your job duties and responsibilities, you collect personal information about employees or other people such as clients or customers, you must comply with this policy. This includes ensuring the information is processed in accordance with GDPR, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary.

You must also comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject (unless prior written consent has been given). Particularly, it should not be:
  1. given to someone from the same family
  2. passed to any other unauthorised third party
  3. placed on the Company's website
  4. posted on the Internet in any form

- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.

- Where <insert dealership> provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard.

- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.

- If you receive a request for personal information about another employee, you should forward this to the Data Protection Officer who is responsible for dealing with such requests.

- Ensure any personal data you hold is kept securely (i.e. where an unauthorised individual finds it impossible to access this data), either in a locked filing cabinet or if computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.

- Do not access another employee's records without authority as this will be treated as gross misconduct and it is a criminal offence.

- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject.

- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.

- Ensure that, when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and GDPR, in particular in matters of data security.

- Ensure that hard copy personal information is disposed of securely

Internal Employee Data Protection Policy

- Remember that compliance with GDPR is your personal responsibility. If you have any questions or concerns about the interpretation of these rules, please contact the Data Protection Officer immediately.

Please sign and return the declaration to <Data Protection Officer>.

Employee Declaration

I have read and understood the Data Protection Policy and understand that my personal data will be processed and stored by <insert dealership> for payroll and human resources administration.

Employee Name: _____ **Mobile Number:** _____

Email Address: _____ **Department:** _____

Signed: _____ **Date:** _____

Data Protection Officer

Name: <Insert Full Name>
Address: <Insert Dealership Postcode>
Email: <Insert Email Address>