

In accordance with the UK General Data Protection Regulation (UK GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees, workers and contractors of Carter Group. Carter Group is our brand name and we have two separate trading companies Carter Security Limited and Carter Services Group Limited. Carter Security Limited is a Security & Fire Systems provider registered in England & Wales (Company Number 07474907) ("we", "us", "our" or "CARTER SECURITY") with registered office at Unit 14 Saffron Court, Southfields Business Park, Basildon, Essex SS15 6SS. Carter Services Group Limited is an Electrical Contractor registered in England & Wales (Company Number 11489438) ("we", "us", "our" or "CARTER SERVICES GROUP") with registered office at Unit 15 Saffron Court, Southfields Business Park, Basildon, Essex SS15 6SS.

A) DATA PROTECTION PRINCIPLES

Under UK GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- a) processing is fair, lawful and transparent
- b) data is collected for specific, explicit, and legitimate purposes
- c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
- d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- e) data is not kept for longer than is necessary for its given purpose
- f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- g) we comply with the relevant UK GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

- a) personal details such as name, address, phone numbers
- b) name and contact details of your next of kin
- c) your photograph
- d) your gender, marital status, information of any disability you have or other medical information
- e) right to work documentation
- f) information on your race and religion for equality monitoring purposes
- g) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter
- h) references from former employers
- i) details on your education and employment history etc
- j) National Insurance numbers
- k) bank account details
- l) tax codes
- m) driving licence details and DVLA checks carried out six monthly
- n) criminal convictions – Basic and/or Enhanced disclosure are required to meet the performance of your employment contract
- o) information relating to your employment with us, including:
 - i) job title and job descriptions

- ii) your salary
- iii) your wider terms and conditions of employment
- iv) details of formal and informal proceedings involving you such as; letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
- v) internal and external training modules undertaken
- vi) information on time off from work including sickness absence, family related leave etc
- p) CCTV footage
- q) Company ID and building access card records
- r) IT equipment used including telephones and internet access
- s) GPRS tracking devices within vehicles and lone working devices

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the employment contract that we have entered into with you e.g. using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
5 Year Screening and Basic Disclosures checks	Performance of the Contract
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g. promotion	Our legitimate interests
Making decisions about salary and other benefits	Our legitimate interests
Ensuring efficient administration of contractual benefits to you	Our legitimate interests
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests
Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained	Our legitimate interests
Implementing grievance procedures	Our legitimate interests

Assessing training needs	Our legitimate interests
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests
Managing statutory leave and pay systems such as maternity leave and pay etc	Our legitimate interests
Business planning and restructuring exercises	Our legitimate interests
Emails are strictly for business use and treated as written documents	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

- a) health
- b) sex life
- c) sexual orientation
- d) race
- e) ethnic origin
- f) political opinion
- g) religion
- h) trade union membership
- i) genetic and biometric data.

We carry out processing activities using special category data:

- a) for the purposes of equal opportunities monitoring
- b) in our sickness absence management procedures
- c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

- a) you have given explicit consent to the processing
- b) we must process the data in order to carry out our legal obligations
- c) we must process data for reasons of substantial public interest
- d) you have already made the data public.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract of employment with you. This could include being unable to offer you employment, or administer contractual benefits.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis of performance of the contract to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with UK GDPR.

Data is shared with third parties for the following reasons:

Peninsula for the administration of holidays, sickness records and HR related issued;
Accountant relating to payroll or tax issues;
Nest Pensions relation to financial pension contributions,
Screening Company (currently SVS) that will carry out security screening and basic disclosures at recruitment stage; and
Insurance Company if the event of a claim related issue or to fulfil a legal obligation,
External Auditors for the purpose of evidence demonstration of our legal obligations,
Morcan IT for the purposes or implementing IT systems, ongoing monitoring of system performance and keeping our systems cyber secure,

we may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us. We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. Retention periods can vary depending on why we need your data, as set out below:

Record	Statutory Retention Period
Children/young adults	Until the child reaches 21
Retirement Benefits Schemes	6 years from the end of the scheme year
Statutory Maternity Pay (calculations, certificates, medical evidence)	3 years after the end on the tax year in which the period ends
Wage/salary (overtime, bonuses, expenses)	6 years
National Minimum Wage	3 years after the end of the consequent pay reference period
Working hours	2 years after they are made

Record	Recommended Retention Period
Application forms and interview notes	6 months to a year or for the period of your employment
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	Until child is 18 (birth/adoption)

Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after end of benefit
Personnel files, training records (disciplinary records, working time records)	6 years after end of employment
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years after date of redundancy
Statutory Sick Pay records, calculations, certificates, self-certificates	at least 3 months after the end of the period of sick leave, but 6 years after the employment ceases advisable
Time cards	2 years after audit
Trade Union agreements	10 years after end
Works Council minutes	Permanently

K) AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

- a) the right to be informed about the data we hold on you and what we do with it;
- b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
- c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
- d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
- e) the right to restrict the processing of the data;
- f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
- g) the right to object to the inclusion of any information;
- h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under UK GDPR.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is: Krystal Simmonds, Company Secretary, 020 3637 3555 or admin@carter-group.co.uk.

PRIVACY NOTICE FOR EMPLOYEES



Issue Record

Version No	Review	Date
V1	Original issue	22/05/2018
V1	Reviewed	30/01/2019
V2	Carter Group.	03/02/2020
V2	Reviewed.	03/02/2021
V3	UK GDPR implementation and review.	24/01/2022
V3	Reviewed.	31/01/2023
V3	Reviewed.	21/02/2024
V4	Reviewed.	21/02/2025

Signed:

A handwritten signature in blue ink, appearing to read "Danny Cosker".

Danny Cosker, Managing Director
Carter Services Group Limited & Carter Security Limited

21st February 2025