GDPR - DATA PROTECTION POLICY

7th January 2025

FSS GROUP

Est 2006

Field Support Services Group Ltd
Company Registration: 10202947
VAT: 329 6435 79
NCAGE: U1P58
DUNS: 2218833136

44 Bridge Street
Hereford HR4 9DG
United Kingdom

Tel +44 1432 850019
email: hereford@fss-gp.com
web: www.fss-gp.com

Table of Contents

INTRODUCTION

This Data Protection Policy is the overarching policy for data security and protection for the Field Support Services Group (hereafter referred to as “Field Support Services Group”, "us", "we", or "our").

This privacy policy ("policy") will help you understand how Field Support Services Group, uses and protects the data you provide to us.

We reserve the right to change this policy at any given time, of which you will be promptly updated.

Purpose

Supporting the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality, and all other pertinent national legislations is the aim of the data protection policy. We embrace the concepts of data protection by design and by default and acknowledge data protection as a fundamental right.

This policy covers:

Our dedication to common law and legal compliance, as well as our data protection principles;

Protocols for both default and design-based data protection.

What User Data We Collect

When you visit our webpage, we may collect the following data:

- Your contact information and email address.
- Information relating to contracted services.
- Data profile regarding your online behaviour on our webpage.

Why We Collect Data

We are collecting your data for several reasons:

- To facilitate contracted service provisions and understand your needs.
- To improve our services and products.

Legal Basis for Processing Personal Data (GDPR)

We process your personal data based on the following legal grounds:

- Your consent, which you may withdraw at any time.
- The necessity for the performance of a contract with you.
- Compliance with a legal obligation.

Scope

This policy covers all of the data that we process, whether it be digital or hard copy, including special kinds of data.

All employees, including contract workers and temporary employees, are subject to this policy.

Principles

We will be open and honest about the care and treatment of service users and those who are lawfully acting on their behalf.

We will establish and uphold policies to guarantee adherence to the Human Rights Act of 1998, the Data Protection Act of 2018, the General Data Protection Regulation, the common law duty of confidentiality, and any additional relevant legislations.

All applicable regulations and public consent will be taken into consideration as we create and uphold policies for the appropriate and controlled sharing of staff and service user data with other parties.

In cases where consent is required for the processing of personal data, we will make sure that informed and explicit consent is acquired and recorded in an appropriate format and in easily comprehensible language. The person has been informed of the procedures to

withdraw consent. Withdrawal of Consent procedures, and they can do so at any time. We guarantee that withdrawing consent is as simple as giving it.

We will undertake / commission annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed in a clear, equitable, and legal way;
- Collected for specified, explicit and legitimate reasons and not further processed in a manner that is incompatible with those goals;
- Adequate, relevant, and kept to a minimum given the objectives for which they are processed (also known as "data minimisation");
- Accurate and continuously updated;
- Stored for a period of time that allows data subjects to be identified for no longer than is required for the purposes for which the personal data are processed (a practice known as "storage limitation");
- Processed in a way that guarantees the personal data is appropriately secured.

We uphold the personal data rights outlined in the GDPR:

- The right to be informed;
- The right of access;
- The right to be corrected;
- The right to deletion;
- The right to limit processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.
- Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale.
- Nonetheless, to ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to be our Data Security and Protection Lead. The Data Security and Protection Lead will report to the highest management level of the organisation.
- We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

Safeguarding And Securing The Data

Field Support Services Group is committed to securing your data and keeping it confidential. Field Support Services Group has done all in its power to prevent data theft, unauthorized access, and disclosure by implementing the latest technologies and software, which help us safeguard all the information we collect online.

Our Cookie Policy

Please note that cookies don't allow us to gain control of your computer in any way. They are strictly used to monitor which pages you find useful and which you do not so that we can provide a better experience for you.

If you want to disable cookies, you can do it by accessing the settings of your internet browser. You can visit https://www.internetcookies.com, which contains comprehensive information on how to do this on a wide variety of browsers and devices.

Data Protection By Design And By Default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

- We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
- It is unlikely that any small organisation will be required to undertake a data protection impact assessment. Though it is considered best practice to do one for your care plans at a minimum. Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA).
- All new systems used for data processing will have data protection built in from the beginning of the system change.

- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

RESPONSIBILITIES

Our designated Data Security and Protection Lead is The Administrative Manager. The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;
- To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management to fulfil this work.

OUR DATA PROTECTION PROCEDURES

Data Back Ups

Field Support Service Group conducts data back ups regularly. When using external storage devices, these are encrypted and locked in secure filing cabinets when not in use. Back-ups are not connected to any live data source.

Strong Passwords And Multi-Factor Authentication

Field Support Service Group use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored.

Where possible, multi-factor authentication is used. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message.

Filtering Suspicious Emails

FSS training and induction includes how to spot suspicious emails. Team members are trained to look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated.

Anti-Virus And Malware Protection

Anti-virus software can help protect devices against malware sent through a phishing attack. All Field Support Services Group devices yare secured with the latest software.

Protecting devices when unattended

Field Support Service Group training and induction includes advice on securing devices - Lock your screen when you're temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer and at the end of each working day put it in a secure locked cabinet.

Wi-Fi connection is secure

Using public Wi-Fi, or an insecure connection, could put personal data at risk. Field Support Services Group use a secure connection in its offices when connecting to the internet. If using a public network, staff are advised to use a secure Virtual Private Network (VPN).

Limit access to those who need it

Different employees use different types of information. Field Support Services Group has implemented access controls to make sure people can only see the information they need. For example, payroll or HR may need to see workers' personal information, but operations staff do not.

If an employee leaves the company, or are absent for a long period of time due to sickness etc, Field Support Services Group will suspend their access to company systems.

Minimising Data Storage

Regularly removing data that is no longer required by the company reduces the amount of personal information at risk in the event of a cyber-attack or personal data breach.

Dispose of old IT equipment and records securely

Field Support Services Group ensures no personal data is left on computers, laptops, smartphones or any other devices, before professionally disposing of them. The company uses deletion software and contracted specialists to fully remove stored data.

Approval

This policy has been approved by the Field Support Services Group, Higer Management Team and will be reviewed at least annually.