Data Protection Policy

Purpose

Churches Fire Security Limited (We/The Company) is committed to protecting and respecting your privacy. This policy (together with our Terms and Conditions and any other documents referred to within) sets out the basis on which any personal data we collect form you, or that you provide to us, will be processed by us. The Company is under an obligation to protect the confidentiality of information held and to ensure that personal data is not divulged to others, unless in doing so it strictly follows the purpose for which the information was supplied. The Company complies with GDPR requirements.

This policy defines how Churches Fire Security Limited identifies the source of the personal data it holds, what that personal data is and how that data is then processed, by what means and by whom. This policy also defines how Churches Fire Security Limited protects the interests of Data Subjects in preventing Data Breaches, identifying when they do happen and what action it takes post breach. This policy also defines how an applicant can make a request for their personal information under the GDPR. This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information.

Scope

1. This policy applies to all Churches Fire Security Limited customers, employees, management, contractors, and persons with authorised access to personal data.
2. This policy applies to personal data of job applicants, employees, workers, suppliers, contractors, volunteers, interns, apprentices and former employees, who must be familiar with this policy and comply with its terms.
3. This policy describes how Churches Fire Security Limited intends to identify what personal data it processes, under what basis it does so, how it is processed and by who, when it is processes and what the reasons for processing are.
4. This policy describes how Churches Fire Security Limited intends to put procedures in place to prevent Data Breaches and what the process is when a Data Breach is discovered.
5. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by employees will be taken seriously and may result in disciplinary action including dismissal and precaution.

Policy Statement

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information for our own business and administrative purposes (including employee

Data Protection Policy

administration and sales) and on behalf of our clients / customers. We recognise the need to treat all information in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers and our clients / customers and for our own business and administrative purposes as a data controller. We also undertake processing as a data processor on behalf of our clients/ customers in the course of providing our services to them. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and other regulations. GDPR imposes restrictions on how we (and our customers) may use that information.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by employees will be taken seriously and may result in disciplinary action including dismissal and prosecution.

Definitions

Churches Fire Security Limited	*Churches Fire Security Limited* as the company to which this policy applies
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems.
Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments - Monitoring staff conduct, disciplinary matters - Marketing our business - Improving services
Personal Data / Data Subject	means any information relating to an identified or identifiable living person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

Data Protection Policy

	such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Sensitive Personal Data.	includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned. - any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	are the people who or Company's which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. We are the data controller for all processing that we do for our own business and administrative purposes (including employee and supplier management) but not for the processing that we do on behalf of client / customers.
Data Processors	include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf. We act as a data processor when we process personal data on behalf of our customers in the course of providing the services ("our services") to them.
Data Users	include our employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
Processing	is any activity that involves use of the data whether or not by automated means. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our company is [the Information Commissioners Office].
GDPR	The General Data Protection Regulation
Data Breach	An incident in which personal data belonging to a Data Subject has potentially been viewed, stolen or processed by an individual, organisation or State that is unauthorised to do so.

Data Protection Policy

Responsibilities

Executives/Management

- Maintain this Policy.
- Approve this Policy.
- Authorise training for all staff, contractors and persons that are directed to use Personal Data by Churches Fire Security Limited.
- Enforce sanctions.
- Designate Data Protection Officer or equivalent to oversee.
- To ensure that adequate Data Security measures are in place and reviewed to protect Data Subjects.
- To act immediately on Data Breaches where directed to by the Data Protection Officer.
- The executives hold overall responsibility for Subject Access Requests but can delegate day to day operational responsibility to others in the organisation.

Data Protection Officer

- Responsibility for the execution and maintenance of this agreement.
- To review all potential Data Breaches that are reported by the Designated Data Protection Lead.
- To qualify the potential Data Breach and follow published process as required.
- Review Schedule.
- Document what Data Subjects are being processed.
- Identify where personal data that is processed by Churches Fire Security Limited has originated.
- Establish what type of consent the Data Subject has given for the processing of their data by Churches Fire Security Limited.
- Define why the Data Subjects personal data is being processed.
- Identify how long personal data is processed.
- Produce documentation that allows Churches Fire Security Limited to confidently identify all personal data that is processed and under what conditions it is processed and meet their GDPR obligations.
- The DPO has executive responsibility for the management of Subject Access Requests; this includes dealing with complaints from the Information Commissioners Office, general.

Director, Training

- Training of all persons to which this policy applies.

Data Protection Policy

Employee responsibilities

- Understand and comply with the Company's policies regarding 3rd Party Data Processors.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) Processed fairly and lawfully.
b) Processed for limited purposes and in an appropriate way.
c) Adequate, relevant, and not excessive for the purpose.
d) Accurate.
e) Not kept longer than necessary for the purpose.
f) Processed in line with data subjects' rights.
g) Secure.
h) Not transferred to people or companies / organisations situated in countries without adequate protection.

The Lawful Basis on Which we Use This Information

In accordance with article 6 of the GDPR we will only process data for the performance of a contract to which the data subject is a party.
In accordance with article 9(2) of the GDPR we will only process special category data where processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

Customer and Vendor Records

You may give us information about you by filling in forms on our site www.Churches Fire.com (our site) or by corresponding with us by phone, e-mail or otherwise. This includes information you provide when you enter into a service or supply contract with us, search our site for a product or completion of an enquiry form on our site.
Data is provided by the data subject, or via acquisition of another company. This is limited to:
Company Name Invoicing Address Service Site Address Contact Names Contact Telephone Numbers Company Email Addresses

Churches Fire
COMPLETE FIRE & SECURITY

Data Protection Policy

Contact Records

The company will keep a record of contacts we receive through the course of our business. This is to ensure we can respond to the inbound enquiries.

Employee Records

In order to manage the business Churches Fire keeps the following records about employees:

Name, Date of Birth, Sex, Address, Personal Telephone Number, Personal Email Address, Ethnicity, Identity Documents for Right to Work (Passport, birth certificate), Medical History, Next of Kin, Sickness record, Disciplinary Record, CV, Qualifications, Rate of pay, Bank Details, Performance Record, Appraisals, Criminal Records and References.

Churches Fire will ensure that all employee records will be kept accurate and up to date. The records will be kept secure and access limited to necessary personnel who have a level of authority. Limited information may be passed to third party training providers to ensure you are qualified to a level required to carry out your job.

The Company will respect employees' privacy and will not disclose personal information without the employee's specific consent, unless there is some other justification or legal requirement to do so.

We will inform employee's when we have a legal duty to pass personal information on to a third party, for example HM Revenue & Customs.

Emails

Emails are retained for one year for each user. After one year, emails are archived by a system called Mimecast. This system will retain records for a further 6 years but access only available to IT to retrieve mail. Emails produced using your Company email account are the property of The Company and as such are monitored therefore no personal information pertaining to the user can be exempt if we wish to view it.

Fair and Lawful Processing

GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is when processing data (for our own administrative purposes, this is Company Name), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred. Customers or partners should provide this information to data subjects when they act as data controllers and we process personal data on their behalf as a result of providing access and use of our services.

Churches Fire
COMPLETE FIRE & SECURITY

Data Protection Policy

For personal data to be processed lawfully, the data controller must ensure that certain conditions have been met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. This responsibility lies with other controllers when we process personal data on their behalf.

Adequate, Relevant and Non-Excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. This responsibility also lies with schools when we process personal data on their behalf.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out of-date data should be destroyed. We expect other data controllers to ensure that any data that we process on their behalf is accurate and up to date.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. We also expect other controllers and processors to ensure that personal data is not kept for longer than is necessary.

Processing in Line With Data Subjects' Rights

Data must be processed in line with data subjects' rights.

Churches Fire
COMPLETE FIRE & SECURITY

Data Protection Policy

Data subjects have a right to:

- Be informed about the collection and use of their data.
- Request access to any data held about them by a data controller.
- Request to restrict or supress the use of their personal data.
- Ask to have inaccurate data amended.
- Have their personal data erased 'the right to be forgotten'
- Data portability to obtain and reuse their data for personal use across multiple services.
- Object to processing based on legitimate interests, profiling and direct marketing or scientific, historical or statistical use.
- Information regarding any automated decision making and profiling.

We may, from time to time, need to provide other controllers or processors with assistance to enable them to respond to any such assertion of these rights by data subjects.

Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

When we act as a data controller (in respect of the personal data we hold for our own administrative purposes), GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves. When we process personal data on behalf of other controllers, our obligations concerning data security are imposed through our contract with the data controller.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- "Confidentiality "means that only people who are authorised to use the data can access it.
- "Integrity" means that personal data should be accurate and suitable for the purpose for which it is processed.
- "Availability" means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on a central computer system (cloud or on premise) instead of individual PCs.

Security Procedures Include:

"Entry controls." Any stranger seen in entry-controlled areas should be reported.

Data Protection Policy

"Secure lockable desks and cupboards." Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

"Equipment." Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended. Portable electronic devices should not be left unattended.

Confidentiality

The Company has a duty to ensure that all its affairs and information held on behalf of and relating to its data subjects is kept confidential. This is managed by access limited to those who need the data to fulfill the contract, review of internal procedures and audits of those procedures.

Conflict of Interest

It is a requirement of your employment that you will not engage in activity, which impairs, or might reasonably be thought by the Company to impair, your ability to act in its best interests. This includes, but is not limited to, working in any way for any person or organisation which the Company may reasonably believe to be in competition with it. If you are in any doubt as to what you may or may not do you should refer to your manager. You are required to inform you manager if you have additional employment.

Staff may carry out private work in their own time provided that:

- It does not adversely affect their work for Churches Fire
- It could not lead to suspicion or favour or influence in relation to any contracts from Churches Fire
- It is not contrary to the interests of Churches Fire, in particular any work that indirectly or directly competes with Churches Fire
- Staff do not use their position in Churches Fire to make any private gain
- No fee should be accepted in return for any favour to any Company or individual
- Any fees for work/lectures/interviews undertaken in normal working hours should be paid into Churches Fire funds, unless agreed otherwise by a Company Director.

Dealing with Subject Access Requests

The General Data Protection Regulation (GDPR) gives individuals (Data Subjects) rights of access to their personal records held by Churches Fire Security Limited.

Churches Fire Security Limited regards the General Data Protection Regulation as an important mechanism in achieving an honest and safe relationship with its

Data Protection Policy

clients, prospective clients and employees. The General Data Protection Regulation entitles an individual, with certain exceptions, to a copy of both manual data recorded in a relevant filing system and computer data relating to them together with reasoning's as to why it is being processed and the sources and destination of the data. A request for such information under the GDPR is known as a Subject Access Request. All records that contain personal data of individuals held and maintained by Churches Fire Security Limited will be subject to the General Data Protection Regulation.

A formal request from a data subject for information that we hold about them (either for our own purposes, or on behalf of another controller or processor) must be made in writing. A fee may be payable by the data subject for provision of this information where unreasonable cost is incurred in processing the request. Any member of staff who receives a written request should forward it to their manager immediately.

Providing Information Over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular, they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked. When the request relates to personal data that we process on behalf of another controller or processor, the caller should direct their request to the relevant party.
- Refer to their manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Any member of staff taking credit card payments over the phone will ensure that they stop the call recording whilst taking credit card details.

Individual Responsibilities

Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the company know if data provided to the company changes, for example if an individual moves to a new house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients during their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the company relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Data Protection Policy

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Data Breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Churches Fire
COMPLETE FIRE & SECURITY

Data Protection Policy

Data Mapping

Data mapping allows us to:

- Understand the information life cycle of sensitive information for key processes throughout the business.
- Evaluate the strength and effectiveness of controls and safeguards.
- Create a master repository of information life cycle details, including data element types, collection mechanisms, transfers, privacy and security practices and transfers to third parties.
- Establish a sensitivity index to focus control enhancements on areas of highest privacy and security risks.

Impact Assessments

Some of the processing that the company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Sanctions

Any non-compliance of this policy by any person appointed by Churches Fire Security Limited will be subject to the Company's disciplinary process.

Additional Notes

This policy does not form part of the formal contract of employment or contract for services, but it is a condition of employment or engagement that employees, workers or contractors will abide by the rules and policies made by the Company.

The Company reserves the right to review this policy at any time and to make such changes as it considers appropriate. If this is necessary in order to reflect changes in legislation, such changes or terminations may be made without advance notice.

Monitoring and Review of the Policy

We will continue to monitor and review the effectiveness of this policy to ensure it is achieving its stated objectives.

The Company reserves the right to review this policy at any time and to make such changes as it considers appropriate. If this is necessary in order to reflect

Data Protection Policy

changes in legislation, such changes or terminations may be made without advance notice.

Further Information

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

If you would like further information about this policy, please contact our Data Protection Officer:
Natalie Potter of Churches Fire Security Limited, Fire House, Mayflower Close, Chandlers Ford, Southampton, SO53 4AR. Our registration number is **Z2121232**

Date of review: 14/07/22
Next review date: 14/07/23