

# Privacy Policy

This privacy policy explains how and why we use your personal data, to make sure you stay informed and are confident about giving us your information.

## Who are we?

Throughout the policy the words ‘we’, ‘us’ or The Company refers to Incentive FM Group Ltd (including Incentive FM Ltd, Incentive QAS Ltd, Incentive Tec Ltd, SWC Ltd, Incentive Tec Fire & Security Ltd, Incentive FM Consultancy Ltd “the Company”

Incentive FM Group Ltd is committed to keeping your information secure and managing it in accordance with our Privacy Policy, shared only with third parties by request or in the execution of our services.

## Scope:

This policy applies to all data subjects whose personal data is collected and used by Incentive FM Group Ltd and subsidiaries. This Privacy Notice explains how we collect, use and look after your personal information including when you visit our website and your rights with regard to this.

“website” means the website you are using ([www.incentive-fmgroup.com](http://www.incentive-fmgroup.com)) and any subdomains of this site (e.g. Incentive-fm.com, Incentive-qas.com) unless expressly excluded by their own terms and conditions. It does not extend to any websites that can be accessed from this website including, but not limited to, any links we may provide to social media websites.

## Responsibilities:

Data controller: The Company

The Data Protection Officer is responsible for ensuring this notice is made available to data subjects.

The General Data Protection Regulation (GDPR) requires employers to be transparent about the personal data that they hold and how it is used. The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

## What information does the Company collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;

- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Company collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

The Company seeks information from third parties with your consent only.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

## Why does the Company process personal data?

The Company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlement as appropriate to your role.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Company to:

- run recruitment and promotion processes;
  - maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
  - operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
  - operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
  - operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
  - obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
  - operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
  - ensure effective general HR and business administration;
  - provide references on request for current or former employees;
  - respond to and defend against legal claims; and
  - maintain and promote equality in the workplace.
- Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow the organisation to communicate appropriately and process fees if applicable.

Where the company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the Company uses for these purposes is anonymised or is collected with the express

consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

## Who has access to data?

Your information will be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The Company shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The Company may also share your data with third parties in the context of a TUPE transfer or sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

We may pass your personal data on to third-party service providers contracted to the Company in the course of dealing with you or if legally required to do so e.g in connection with payroll, the provision of benefits, company vehicles and the provision of occupational health services.. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfill the service they provide to you on our behalf. Where third parties are involved we will have a contract in place to ensure that the nature and purpose of the processing is clear, that they are subject to a duty of confidence in processing your data and that they will only act in accordance with our written instructions.

The Company will not transfer your data to countries outside the European Economic Area.

## How does the Company protect data?

The Company takes the security of your data seriously. The Company has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality, are obliged to implement appropriate technical and organisational measures to ensure the security of data and comply with the General Data Protection Regulation and have robust systems and processes to protect the security of your information.

## For how long does the Company keep data?

The Company will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are in the attached Appendix

## Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact the Data Protection Officer (contact details are shown below). You can make a subject access request by completing the organisation's form for making a subject access request.

### Reporting a concern to us or to the Information Commissioner's Office

If you have a concern regarding how we handle your personal data then we kindly request that you inform us about it first so that we can work with you in an effort to resolve it.

You can report a concern or raise a complaint with us initially by contacting your usual contact or speaking to a member of staff on 0207 979 7769 who will put you in contact with the data protection manager or email [dataprotection@incentive-fm.com](mailto:dataprotection@incentive-fm.com)

Alternatively, you can write to us by sending your letter to:

Data Protection Officer  
44 Loman Street  
London  
SE1 0EH

We aim to acknowledge your complaint within two business days and provide a resolution within 28 days. If we are unable to meet this timescale we will write to notify you in advance.

If you are not satisfied with our proposed resolution to your complaint you can raise the matter directly with the Information Commissioner's Office (ICO). The ICO will take steps to address your concern and provide guidance and support to us so that we can put things right.

Details as to how to get in touch with the ICO or report a concern can be found on their webpage

<https://ico.org.uk/concerns/>

Tel: 0303 123 1113  
Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

## What if you do not provide personal data?

You have some obligations under your employment contract to provide the Company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the Company's ability to administer the rights and obligations, arising as a result of the employment relationship, efficiently.

The Data Protection Officer is the owner of this document and is responsible for ensuring this is reviewed in line with the requirements of GDPR.

A current version of this document is available on the company website

### Signature



**Martin Reed**  
**Chief Executive**  
**Date: 11<sup>th</sup> January 2021**

# Appendix 1

## Retention of data

Record	Statutory period
--------	------------------

### HR

Training records	6 years
Staff contact details	3 years
Payroll records	3 years
Pension records	6 years
Medical records	3 years *
SIA records	3 years
Right to work checks	3 years
Application Forms	3 years

\*5 years if related to workplace incident

### Unsuccessful candidates

Application forms	6 months
-------------------	----------

### Finance

Staff payroll	7 years
Expenses	7 years

### Health & Safety

Accident, Incident & Near Miss records	5 years
Health & Safety Training records	Indefinitely
DSE assessments	5 years
Risk Assessments	5 years