OUTCOMES FIRST GROUP – PRIVACY NOTICE

PERSONAL DATA BELONGING TO **EMPLOYEES**, INCL. APPLICANTS, BANK AND AGENCY STAFF

This document is an addendum to the Outcomes First Group Privacy Notice, providing further details on the processing of data belonging to our employees, including bank and agency staff, as well as those going through the employment application processs.

Please note that for data protection purposes, 'Processing' means collection, recording, organising, structuring or storing, adapting or altering, retrieving, consulting or use, disclosing by transmission, disseminating or otherwise making available, aligning or combining, or restricting, erasing or destroying personal data.

The personal data we process

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- *Contact details
- *Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Information from your Disclosure and Barring Service (DBS) or Disclosure Scotland checks including any information regarding criminal convictions
- Bank account details, payroll records, National Insurance Number and tax status information
- *Recruitment information, including copies of ID, right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- *Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage and key fob monitoring
- Data about your use of the service's information and communications system
- Any data transferred to us under TUPE Regulations.
- Vehicle telematics
- Employment perquisites and benefits

We may also collect, store and use information about you that falls into 'special categories' of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Physical and mental health, including any medical conditions, and sickness records
- Criminal convictions and DBS referrals

Applicants (*)

We obtain and hold applicant data as part of the recruitment process (see **items* listed above), as required by Safer Recruitment best practice and in accordance with this Privacy Notice. Personal data belonging to unsuccessful applicants will be held in accordance with the period set out in our personal data retention schedule. For successful candidates, the on boarding process will ensure the remaining records are completed as per our employer obligations and will be processed in accordance with the minimum period set out in our personal data retention schedule .

Agency Staff

Agency staff are employed by their agency company, who are also Data Controllers in their own right concerning the handling of personal data belonging to staff connected with their agency. As a joint Data Controller, however, Outcomes First Group will require certain documentation to be shared by the agency or agency staff member for safeguarding reasons and to ensure that we have the data and documents required to be satisfied of the various statutory regulations to which we are subject.

Why we use this data

The purpose of processing employee data is to help us run our services and comply with our legal obligations in doing so, which includes to:

- Enable staff and contractors to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards the people we support
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the regulatory bodies and professional associations.
- Process insurance claims
- Comply with our legal obligations
- To safeguard children and vulnerable adults
- To bring or defend legal proceedings
- To support law enforcement when required to do so
- To obtain or permit others to obtain legal advice

For certain roles, we have a legal requirement to undertake Disclosure and Barring Service checks (DBS, England and Wales) or a Disclosure Scotland check. Where we do so, we only do so in accordance with our legal requirements, as updated from time to time. We comply fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information. In accordance with insurance requirements, DBS certificate numbers will be retained for 50 years.

Our lawful basis for using this data

We only collect and use personal information about you when the Law permits it.

Most commonly, we use it:

- To fulfil a contract we have entered into with you or to take steps at your request before entering into a contract
- To comply with legal or regulatory obligations
- Where we, or a third party have a legitimate interest in processing your information
- To carry out a task in the public interest

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and we will explain how you can withdraw consent easily if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap and there may be several grounds that justify the company's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you (or your agency), we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in line with our Data Retention & Disposal Policy and Schedule, which is available to all staff as part of the policy library.

We create and maintain an employment file for each employee on Cascade (online, secured staff portal) or Reach (recruitment system for applicants). The information contained on these systems is secure and is only used for purposes directly relevant to recruitment and employment. Services have separate arrangements for securely holding selected data on agency staff as the majority of personal information remains stored by the agency as the employer.

Once your employment/contract with us has ended (or after 6-12 months for unsuccessful applicants), we will retain these records or delete information in accordance with our Data Retention & Disposal Policy and Schedule, which set out how long we keep information and refers to the guidance outlined by the relevant regulatory bodies and professional associations.

Data sharing

We do not share information about you with any third party without your consent or liaison with your agency (if applicable), unless the Law permits or requires us to do so. Where it is legally required, or necessary and it complies with data protection law, we may share personal information about staff with:

- *Local authorities – to meet our legal obligations to share certain information with it, such as safeguarding concerns*
- *Regulators*
- *Your family or representatives*
- *Assessors and Examining Bodies*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll*
- *Financial organisations*
- *Central and local government, including Disclosure & Barring Service (DBS)*
- *Our auditors*
- *Survey and research organisations*
- *Trade unions and associations*
- *Health authorities*
- *Security organisations*
- *Health and social welfare organisations*
- *Professional advisors and consultants*
- *Our own and third party solicitors and legal advisors*
- *Our insurance companies*
- *Charities and voluntary organisations*
- *Police forces, courts, tribunals*
- *Professional bodies*
- *Employment and recruitment agencies*
- *New employer in accordance with Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246), only where applicable*

Employment references

The company does not disclose any employment references received, under which it is under a duty of confidence towards the author, unless:

- it has the author's consent;
- it is in the public interest to do so;
- there is a legal obligation or Court Order, and then only to the extent of such legal obligation or Order.

If you require a copy of a reference that we have received, you should make a request directly to the referee in the first instance or, failing this, provide the company with the referee's written consent to disclose the reference to you, seek a Court Order or otherwise cite the express legal authority upon which we are obliged to breach our duty of confidence by disclosing the reference.