CONTENTS Page

1.0 INTRODUCTION

This document sets out the Outcomes First Group's policy for all services relating to privacy and data protection legislation and should be read in conjunction with the *Confidentiality Policy*.

Our aims are to ensure that all personal data collected about staff, people we support, parents/carers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

Data protection principles outline that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy states how the company will meet these standards and applies to all personal data, regardless of whether it is in paper or electronic format.

Implementation: It is the responsibility of all line managers to ensure that all staff are aware of and understand this policy and any subsequent revisions.

Compliance: This policy complies with all relevant regulations and other legislation as detailed in the *Compliance with Regulations & Legislation Statement*. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

2.0 DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data Protection Officer	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3.0 ROLES AND RESPONSIBILITIES

Our services process personal data relating to children, service users, pupils, staff, governors, visitors and others, and therefore is a Data Controller and, in some instances, a Data Processor. The organisation is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

Data Protection Officer
Outcomes First Group has engaged *IT Governance Ltd* to provide outsourced Data Protection Officer services, The Data Protection Officer is responsible for advising on all elements of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines, in close liaison with the **Performance & Quality Officer**, who coordinates all compliance activities internally.

The Performance & Quality Officer will provide a quarterly report of data protection activities directly to Board Directors via the Governance Group and, where relevant, report DPO advice and recommendations on all data protection issues.

The DPO also provides the Group with advice and guidance on any responses that it needs to make to privacy rights requests from individuals and acts as the escalation point for individuals whose data each service processes, and for the ICO.

Any breach of data protection regulations is reported to the ICO by the Performance & Quality Officer, in collaboration with the DPO.

The Board of Directors
The Board of Directors have overall responsibility for ensuring that our services comply with all relevant data protection obligations.

Responsible Individuals / Registered Managers / Headteachers
All senior managers act as a representative of the Data Protection Officer on a day-to-day basis within their services and are responsible for the implementation of this policy locally. They must also ensure that staff are aware of the need to report any breaches without delay *(see Data Breach Procedure)* and respond correctly to data subject access requests *(see Data Subject Access Request Policy).*

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the service of any changes to their personal data, such as a change of address
- Contacting the Performance & Quality Officer in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

4.0 COLLECTING PERSONAL DATA & CONSENT

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that each service can **fulfil a contract** with the funding body.
- The data needs to be processed so that the service can **comply with their legal obligations under the relevant regulatory body, e.g. Ofsted, CQC, and CIW.**
- The data needs to be processed to ensure the **vital interests** of the individual, e.g. to protect someone's life.
- The data needs to be processed so that each service, can carry out its official functions in compliance with their funding agreements in place with local authorities which are **public interest organisations.**
- The data needs to be processed for the **legitimate interests** of each service or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a child aged 12 years or under) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing.

Where we offer online services to children or service users, such as Makaton or other communication aids, we intend to rely on consent as a basis for processing, unless the individual does not have capacity to consent. In these cases, the service will comply with the legal requirements outlined in the Mental Capacity Act 2005.

Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the statutory regulations each service is registered with.

5.0 DATA PROTECTION BY DESIGN OR DEFAULT

The principle of data protection by design or default means that we will put measures in place to ensure we have integrated data protection into all of our processing activities, either as part of standard practice or by specifically considering those requirements at every stage of planning. This includes:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- Completing privacy impact assessments where the services processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our service and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

6.0 PRIVACY NOTICES (Article 12)

When personal data is collected from a data subject in accordance with consent guidelines, the company is transparent in its processing of personal data and provides the data subject with the following information as part of a Privacy Notice, using clear and plain language.

- Who is processing the data
- The purpose(s), including legal basis/justification, for the intended processing of personal data

- Potential recipients of personal data
- Any information regarding the intention to disclose personal data to third parties, the safeguards in place for transferring this data and whether it is transferred outside the EU
- Any information on technologies used to collect personal data about the data subject;
- Any other information required to demonstrate that the processing is fair and transparent.

A library of template privacy notices for this personal data processing are stored by the Compliance Team on the SharePoint Portal.

7.0 SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child/service user, parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies (we will seek consent as necessary before doing this);
- Our **suppliers or contractors** need data to enable us to provide services to our staff and service users for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with **law enforcement and government bodies** where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- Where we are registered to provide care services with a statutory body.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children/service users or staff.

Where we transfer personal data to a country or territory **outside the European Economic Area**, we will do so in accordance with data protection law.

8.0 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the service holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email, to the Registered Manager or Headteacher of the service or to the Group Quality and Compliance Team. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Staff must follow the guidance set out in the *Data Subject Access Request Procedure*, but if they receive a request which is not capable of being processed following this guidance, or which contains any anomalies, they must immediately forward it to the Performance & Quality Officer – but only in exceptional circumstances.

Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information outlined in privacy notices, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the service's Registered Manager or Headteacher who will forward this to the Group Quality & Compliance Team. If staff receive such a request, they must immediately forward it to the Quality & Compliance Team.

9.0 CCTV

We use CCTV in various locations around some sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the relevant Head of Service or Regional Manager.

10.0 PHOTOGRAPHS AND VIDEOS

As part of our service provision, we may take photographs and record images of individuals undertaking different activities, but we will not accompany them with any other personal information about the individual to ensure they cannot be identified.

We will obtain written consent from the individual, whether an employee or a person we support, or their parents/carers where applicable, and clearly explain how the photograph will be used.

Uses may include:

- Within service notice boards and in company magazines, brochures, newsletters, etc.
- Outside of the service by external agencies such as the promotion, newspapers, campaigns
- Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

11.0 DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept securely and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access, in accordance with the *Clear Workspace Policy.*
- Where personal information needs to be taken off site, staff must sign it in and out from the service, and the information must be transported in a secure manner (encrypted devices or lockable cases).
- Passwords that are at least 8 characters long containing letters and numbers are used to access service computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, wherever possible, such as laptops and USB devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

12.0 DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the groups behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

13.0 PERSONAL DATA BREACH

Each service will make all reasonable endeavours to ensure that there are no personal data breaches by minimising risks through good working practices outlined in this policy.

In the event of a suspected data breach, staff must follow the *Data Breach Procedure*.

Following a review and if advised by the DPO, we will report the data breach to the ICO within 72 hours. Such breaches in a service context may include, but are not limited to:

- Non-anonymised, sensitive data being published online or disclosed to unauthorised individuals
- Safeguarding information being made available to an unauthorised person
- The theft of a service laptop containing non-encrypted personal data

14.0 TRAINING

All staff are provided with data protection training as part of their induction process to ensure they are able to demonstrate competence in their understanding of all relevant legislation, best practice and how this is practised and implemented throughout Outcomes First Group, particularly with reference to information management and system security.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the organisation's processes make it necessary.

15.0 COMPLAINTS ABOUT DATA PROCESSING

Data subjects may complain about the data processing activities of the organisation, including:

- how their personal data has been processed;
- how their request for access to data has been handled;
- how their complaint has been handled.

They may also appeal against any decision made following a complaint.

Any complaints made in relation to the scope of this policy must be logged on Info Exchange and highlighted to the Quality & Compliance Team, who will liaise with the DPO. Complaints will be handled in accordance with the company's Complaints Policy and following advice from the DPO.

16.0 MONITORING ARRANGEMENTS

The implementation of this policy will be monitored through a regular audit arrangement coordinated by the Performance & Quality Managers, using a standard Data Audit Report template. The report and any actions arising from this audit will be logged on the Info Exchange system, which will track completion of advised improvements by local management. Progress in these areas will be monitored by the Performance & Quality Managers and the Governance Group, who will implement Group-wide procedural changes where patterns of risk are identified.