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 (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

Data protection principles outline that personal data must be:

- Processed lawfully and fairly
- The purpose of processing must be specified, explicit and legitimate
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Kept for no longer than is necessary
- Processed secure manner

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.

## 2.0 DEFINITIONS

| TERM | DEFINITION |
|---|---|
| **Personal Data** | This has the meaning given to it by the UK GDPR and means any information relating to an identifiable, living person. This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>• Photograph<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| **Special Categories of Data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Health – physical or mental<br>Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, viewing, 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 Controller** | A person or organisation who (either alone or jointly with another) determines the purposes and manner in which any personal data is processed. |
| **Data Processor** | A person or organisation 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 are required to manage personal data relating to children, service users, pupils, staff, governors, visitors and other. Therefore, Outcomes First Group acts as a Data Controller in terms of the records we control as well as, in some instances, a Data Processor where the information is controlled by another person/organisation, e.g. paperwork managed by local authorities, healthcare professionals or other agency, and we process the information on their instructions.

The organisation and its subsidiaries, which process personal data, are registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

**Data Protection Officer (DPO)**

The Data Protection Officer, supported by the Data Protection & Regulatory Compliance Team, is Christopher Duffy (data.protection@ofgl.co.uk) who responsible for advising on all elements of this policy, monitoring our compliance with Data Protection Law, and developing related policies and guidelines.

The DPO also provides the Group with advice and guidance on any responses that it needs to make to subject access requests from individuals (data subjects) and acts as the escalation point for individuals whose data each service processes, and for the Information Commissioners Office ('ICO').

Any reportable breach of data protection regulations, which is notifiable under UK GDPR legislation, is reported to the ICO by the Data Protection & Regulatory Compliance Team.

**Board of Directors**

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

**Responsible Individuals / Registered Managers / Headteachers**

All senior managers 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 Procedure).*

**All staff are responsible for:**

- 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 Data Protection & Regulatory Compliance Team 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 of the United Kingdom.
  - 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 6 lawful bases are as follows:

1. **Consent:** The individual has given clear consent for us to process their personal data for a specific purpose (or their parent/carer, when appropriate in the case of a child aged 12 years or under).
2. **Contract:** The processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal Obligation:** The processing is necessary for us to comply with the Law (not including contractual obligations).
4. **Vital Interests:** The processing is necessary to protect someone's life.
5. **Public Task:** The processing is necessary for us to perform a task in the public interest or for our official functions and the task or function has a clear basis in Law.
6. **Legitimate Interests:** The processing is necessary for our legitimate interests, or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

No single basis is 'better' or more important than the others; the basis that is most appropriate to use will depend on the purpose and relationship with the individual.

Special Category Data is personal information that needs more protection due to its sensitivity. In order to lawfully process Special Categories of Data, we must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked. There are 10 conditions for processing special category data in Article 9 of the UK GDPR. Five of these require us to meet additional conditions and safeguards set out in UK law, in Schedule 1 of the DPA 2018.

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 and any associated Codes of Practice issued under it.

When sharing data we will also have regard to the ICO's Data Sharing Code of Practice.

### 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. Our Privacy Notice and linked documents are published on our website.

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 with which each service is registered.

## 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 Data Protection Impact Assessments (DPIAs) 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 and related policies and privacy notices;
- Regularly training members of staff on Data Protection Law, this and related policies, and any other data protection matters, for which attendance records are maintained;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- By achieving and maintaining external Cyber accreditations;
- By taking appropriate organisational and technical measures;
- 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 published Privacy Notice)
  - 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, the company is transparent in its processing of personal data and provides data subjects with the following information as part of a Privacy Notice, using clear and plain language.

- 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 United Kingdom
- 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.

The Outcomes First Group Privacy Notice, including statements for specific data subjects groups, can be found on the company website.

## 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.

As stated above, when sharing personal data, we will have due regard to the ICO's Data Sharing Code of Practice.

**Transferring Data Overseas**

Under UK Data Protection Law, we will only transfer personal data to a country or territory **outside the** United Kingdom, where:

- the UK government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'Adequacy Decision');
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under Data Protection Law.

These are explained below.

**Adequacy Decisions**

We may transfer personal data to certain countries, on the basis of an Adequacy Decision. These include:

- all European Union countries, plus Iceland, Liechtenstein and Norway (collectively known as the 'EEA');
- Gibraltar; and
- Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The list of countries that benefit from Adequacy Decisions will change from time to time. We will always seek to rely on an Adequacy Decision, where one exists.

Other countries or international organisations we are likely to transfer personal data to do may not have the benefit of an Adequacy Decision. This does not necessarily mean they provide poor protection for personal

data, but we must look at alternative grounds for transferring the personal data, such as ensuring appropriate safeguards are in place or relying on an exception, as explained below.

**Transfers with appropriate safeguards**

Where there is no Adequacy Decision, we may transfer personal data to another country or international organisation if we are satisfied the transfer complies with Data Protection Law, appropriate safeguards are in place, and enforceable rights and effective legal remedies are available for data subjects.

The safeguards will usually include using legally approved standard data protection contract clauses.

To obtain a copy of the standard data protection contract clauses and further information about relevant safeguards, please contact the Data Protection Officer.

**Transfers under an exception**

In the absence of an Adequacy Decision or appropriate safeguards, we may transfer personal data to a third country or international organisation where an exception applies under relevant Data Protection Law, e.g:

- you have explicitly consented to the proposed transfer after having been informed of the possible risks;
- the transfer is necessary for the performance of a contract between us or to take pre-contract measures at a data subject's request;
- the transfer is necessary for a contract in data subject interests, between us and another person; or
- the transfer is necessary to establish, exercise or defend legal claims

We may also transfer information for the purpose of our compelling legitimate interests, as long as those interests are not overridden by data subject interests, rights and freedoms. Specific conditions apply to such transfers and we will provide relevant information if and when we seek to transfer personal data on this ground.

## 8.0 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to their personal information that we process. 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 should be submitted wherever possible in writing to ensure clarity of the request, either by letter or email, to the Registered Manager or Headteacher of the service or to the Data Protection & Regulatory 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 Data Protection & Regulatory Compliance Team – but only in exceptional circumstances.

Subject access requests are subject to exemptions, which may be applied following appropriate assessment of the request, and the data collated.

**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 United Kingdom
- 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 Data Protection & Regulatory Compliance Team. If staff receive such a request, they must immediately forward it to the Data Protection & Regulatory 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 as detailed in the *CCTV Policy*.

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 under lock 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.
- 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). Checks on such activities will form part of regular Data Audits.
- 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 in accordance with the *Data Retention & Disposal Policy*. Personal data that is 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 Group's 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 no later than 72 hours after becoming aware of the breach. 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 and refresher training, where changes to legislation, guidance or the organisation's processes make it necessary. Records of all training activities are held by the Talent & Development Team and are available for enquiry as part of Data Audits as 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 Data Protection & Regulatory 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 DPO and the Quality Division, 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 DPO, who will recommend Group-wide procedural changes where patterns of risks are identified.