CONTENTS Page

1.0 INTRODUCTION

This procedure outlines the Outcomes First Group's structured approach to responding to a personal data breach under Article 33 of the General Data Protection Regulation (GDPR), *Notification of a personal data breach to the supervisory authority,* and Article 34*, Communication of a personal data breach to the data subject*.

Implementation: It is the responsibility of all 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 UK General Data Protection Regulation 2018.

2.0 DEFINITIONS

GDPR defines a **personal data breach** in Article 4(12) as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

Personal data is defined under GDPR as "'***personal data'*** *means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier 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*".

A **data security incident** involves a compromise to the security of data, but may not necessarily have led to the disclosure or loss of confidential personal data. It is important to log all incidents in accordance with this procedure, however, as it is not always known at an early stage whether it is a data *incident* or a personal data *breach* which may be reportable to the ICO within a 72 hour timeframe.

The GDPR draws a distinction between a '***data controller'*** (entity which determines the purposes, conditions and *means* of the processing of personal *data)* and a '***data processor'*** (entity which processes personal *data* on behalf of the *controller)* in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

3.0 RESPONSIBILITIES

All Outcomes First Group staff, contractors or temporary personnel ("Staff"), as *data processors*, are responsible for reporting any personal data breach or data incident to their line manager and the Data Protection & Regulatory Compliance Team using the Info Exchange incident reporting system, which acts as the organisation's **Breach Register**. For contractors, who do not have access to Info Exchange, a breach (or potential breach) must be notified to the most senior person with whom they have contact, so that a report may be completed in collaboration with them.

The Info Exchange report is to be completed immediately by any member of Staff who discovers the incident/breach and includes a list of questions designed assess the potential impact of the breach. Analysis and assessment of the nature and severity of the breach is undertaken by the Data Protection & Regulatory Compliance Team, who will provide support to the service and judge whether the matter needs to be raised with the Group's Data Protection Officer and, potentially, reported to the ICO.

4.0 DATA INCIDENT MANAGEMENT PROCEDURE

STAGE 1: REPORTING AN INCIDENT / BREACH (ALL STAFF)

1. Upon identifying any data security incident, staff or other third party must report the matter without undue delay (within same work shift) using the Info Exchange incident reporting system. Staff do not need a log-on for this system to use the remote version of the form: https://optionsgroup.info-exchange.com/events

Please refer to *How to Report a Breach* guidance document for detailed support. A 10-minute video demonstration is also available on Teams (weblink available from the Data Protection & Regulatory Compliance Team, "DP Team"). Items which must be covered in the initial report are:

- Date and time the incident occurred
- The source and reasons for the incident
- How and when the incident was identified
- Exactly what personal information was disclosed (or lost, deleted etc) or nature of the security concern
- If applicable, who the data subject is (initials, how many people) and have they been informed of any breach of their personal information at this stage (if not already informed, please do not communicate with data subjects until advised by the DP Team).
- What the impacts on them are due any breach
- What security arrangements were in place to protect the data (if any) prior to the incident
- What has been done to limit the impact of the incident, e.g. has data been retrieved or incorrect recipient confirmed deletion etc.
- Immediate actions taken to learn from this incident/breach.

2. Full details are recorded on the Info Exchange form (automatically populating the internal Data Incident/Breach Register) and an email alert is immediately sent to the DPO, the DP Team and members of Senior Management.

3. A confirmation email of receipt of this information is generated by Info Exchange to be sent to the reporter to assure them of successful logging of the incident record.

STAGE 2: DATA BREACH IMPACT ASSESSMENT (MANAGERS / DP TEAM)

4. The relevant Manager of the service undertakes an initial assessment of the incident to ensure that any actions possible are taken to secure data/privacy and lessen the impact of the breach.

5. An assessment of the breach is undertaken by the DP Team, who will consult the Data Protection Officer (DPO) where there is a significant risk to the rights and freedoms of the data subjects, or if further guidance is required.

6. The DP Team will discuss the nature of the breach and any remedial action taken with the service and provide further guidance on strengthening data protection practices wherever possible.

7. If all of the above steps have been completed and the DP Team is satisfied that there is no need to notify anyone, the breach record is closed on the Breach Register.

8. Where a personal data breach is assessed as likely to have a negative impact on the data subject(s) and/or involve particularly sensitive information, the DP Team will consult the DPO and agree any steps required under Stages 3 (Notifying ICO & Commissioners) and 4 (Informing Data Subjects) below.

STAGE 3: NOTIFYING THE ICO & LOCAL AUTHORITY COMMISSIONERS (DP TEAM / DPO)

9. Where a breach meets the relevant GDPR criteria, the DP Team will report the breach to the Information Commissioners Office (ICO, supervisory body) without undue delay, and not later than 72 hours after the breach has been identified.

10. If the data breach notification to the ICO is not made within 72 hours, it will be submitted as soon as possible, with a justification for the delay. Any subsequent information that becomes available will also be forwarded without delay.

11. The following information will be provided to the ICO:

- A description of the nature of the breach
- The categories of personal data affected
- Approximate number of data subjects affected
- Approximate number of personal data records affected
- Name and contact details of the DPO and Data Controller representatives
- Known consequences of the breach, both those that have already accrued and those that are likely to occur.
- Any measures taken to address the breach
- Any information relating to the data breach, which may be submitted in phases.

12. In the event the ICO assigns a specific contact in relation to the breach, these details are recorded in the internal Breach Register and actions implemented accordingly.

13. A summary of the breach will also be provided to Commissioner's under the terms of any placement contracts with Local Authorties.

STAGE 4: INFORMING THE DATA SUBJECT (DP TEAM / DPO)

14. If a data breach is likely to result in high risk to the rights and freedoms of the data subject, the company will notify them immediately (or will be advised to do so by the ICO).

15. The notification to the data subject describes the breach in clear and plain language, in addition to information specified in point 11 above.

5.0 DATA INCIDENT MONITORING

Outcomes First Group takes its responsibility for protecting personal data very seriously and senior management will undertake monthly analyses of data incidents and breaches to support risk management and quality improvement work across the company. The DPO will take overall responsibility for monitoring data protection risk management practices.

6.0 INSURANCE

Depending upon the nature of the breach, we may need to notify our cyber insurer. This will be done by the DPO after an assessment of the incident.

APPENDIX: PROCEDURE CHECKLIST

Preparing for a personal data breach:

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.

☐ We know we must inform affected individuals without undue delay.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.