Outcomes First Group

Confidentiality Policy

Policy Folder: Human Resources

CONTENTS Page

1.0 INTRODUCTION

1.1 Outcomes First Group is committed to maintaining the privacy of all colleagues, workers, young adults and children.

1.2 This policy and procedure outlines the responsibility all Employees, Workers and Contract Service Providers to keep confidential, any information relating to anyone working within the organisation or anyone we support , financial dealings and any other information pertinent to the business.

1.3 This policy must be observed by all Employees, Workers and Contractors associated with the Group. Justification for maintaining confidentiality is necessary for a condition of trust.

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

2.0 DEFINITIONS

Word / Term	Descriptor
Confidentiality	Applies to information received through formal channels, informally, or discovered by accident.
Information	In this context is all information relating to the above groups of persons, held in whichever form by, or from the Group employees/workers. It also includes information relating to the Group's business affairs, finances, dealings, transactions and service users.

3.0 PURPOSE

3.1 The purpose of this policy is to assist our Employees and those who work with the Group to understand their duties of confidentiality towards the organisation and the work carried out by Outcomes First Group ('the Group'). The policy also confirms the organisation's absolute commitment to ensuring the confidentiality of any information held by the Group relating to:

- Employees/workers
- looked after children/birth children/ pupils and residents
- stakeholders
- customers
- business partners
- any other information pertinent to the business.

3.2 It is important to ensure that any management action taken is fair and consistent and in keeping with the Outcomes First Group's Equality Policy and practices. Therefore, the policy, procedures and processes identified within this document are applied to all staff irrespective of age, ethnicity, gender, marital or civil partnership status, nationality, offending history, race, disability, religion or belief, sexual orientation, social status, trade union membership or working patterns.

4.0 RESPONSIBILITIES

4.1 The Policy has been produced for the benefit of the Group as a whole; it must be read, and adhered to, by all employees of the Group and by individuals under a contract for service to the organisation.

4.2 It applies to any person authorised by the Group to have access to information.

4.3 Managers are responsible for bringing this to the attention of those working on their behalf.

4.4 All the Group employees' and those working on behalf of the organisation have a statutory obligation to safeguard the confidentiality of personal and sensitive information. This is central to the Group and professional codes of conduct.

5.0 AIMS AND OBJECTIVES

5.1 The terms set out in this Policy, are essential in ensuring that employees, and those contracted to the Group are aware of the information in which they must keep confidential.

5.2 Information pertaining to those in the care and employment of the Group, including, but not limited to:

- Details on local authority children and young people
- Details on pupils or prospective pupils
- Details on historical cases
- Details on customers and suppliers, contractors, freelance
- Details on employee's (including prospective employee's/previous employees e.g., leavers)
- Details on contractors
- Details on stakeholders

5.3 In addition to information pertaining to the Group includes, but is not limited to:

- the Group's business and finances,
- technical procedures and intellectual property rights,
- its customer, client and supplier lists, including details of prospective clients.
- the dealings, transactions and affairs.
- its products and services.
- contact details of clients, customers and suppliers, information about individuals within clients, customers and suppliers.
- financial projections, targets and accounts.
- pricing policies and pricing statistics.
- commercial activities,

- product development and future plans; and
- similar information concerning the Group's clients, customers and suppliers,

5.4 In respect of the above, all of which information is acknowledged to be: -

- Confidential to the Group.
- Commercially sensitive in the Group's market; and
- Potentially damaging to the Group's financial stability if disclosed to a third party.

5.5 Any breach in this duty of confidentiality, will be treated by the Group as gross misconduct, justifying summary dismissal. In the instance of a contractor, or agency worker breaching this confidentiality their contract for services would be immediately terminated.

5.6 It is essential to note that a commitment to confidentiality remains, even when employees (or contractor) has stopped working for the Group.

5.7 If, at any point during their employment, employees or those providing a service, are unsure about points in this policy, or any other, they must discuss the matter with their Line Manager, or Human Resources.

6.0 DATA PROTECTION LEGISLATION

The relevant legislation includes the Data Protection Act 2018 and the General Data

6.0 Protection Regulations 2018, the Human Rights Act 1998, common law and employment law.

6.1 The Data Protection Act 2018 and General Data Protection Regulations 2018 require that an organisation and their employees, or those working on their behalf under a contract for services, having access to personal information or in order to justify accessing such information, must be able to comply with the following principals:

6.2 Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date

- kept in a form which permits identification of data subjects for no longer than necessaryfor the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data

7.0 PRINCIPLES

7.1 The Group expects its Employees, and where relevant contract service providers, to handle personal and business information in a sensitive and professional matter.

7.2 It recognises and defines situations in which information must be shared, e.g., where there is a stronger public interest in information being shared. One such example is child protection/ safeguarding.

7.3 Employees and contract service providers should not gain access, or attempt to gain access, to information to which they are not authorised.

7.4 Information comes into the Group in various ways and stages. From the first point of contact (verbal or written e.g., telephone call, email or fax) the information is privileged and must be kept confidential.

7.5 The Group recognises that protection against breaches in confidentiality can be to keep the numbers of employees and contractors who have excess to particularly sensitive material to a minimum.

7.6 The unauthorised, intentional, or accidental disclosure of confidential information by an employee can lead to disciplinary action, cessation of a contract for services and /or civil proceedings (to restrain individuals from using or disclosing information that may damage the Group). The Group reserve the right to seek damages should any such breach occur.

7.7 The Group, in dealing with the above, will endeavour to ensure that no further breaches of confidentiality take place.

8.0 MAINTAINING CONFIDENTIALITY

8.1 Duties of Employees, and Contracted Service Providers:

8.1.1 To treat information in relation to Employees, young adults, adults and their families/carers and stakeholders, customers and any other information pertinent to the business of the Group in the strictest confidence.

8.1.2 To ensure that information is used, only for the purpose for which it was given, to the Group.

8.1.3 Employee's, workers and contractors/service providers have the individual responsibility to abide by the terms of their contract and the Policies and the Procedures of the Group.

8.1.4 Employee's, workers and contractors/service providers should not access information for which they do not have a proper reason to access in the course of their duties.

8.1.5 Sensitive and confidential information should not be shared with a third party without the prior agreement of a Line Manager, or their delegate or in the case of contract service providers, their contact.

8.1.6 Where Employees are approached by someone they know (or are linked with in anyway) about employment with the Group; advise the person to make their application through the proper channels or refer them through the appropriate scheme, so that the response may be a Company, rather than individual response.

8.1.7 Where Employees are approached by someone they know (or are linked with in anyway) and asked for information that is pertinent to the business of Group they should consult immediately with their Line Manager. They should not under any circumstance give any information; instead they should go through the proper channels, and follow the guidance set out in this policy.

8.2 Duty Of Care

8.2.1 It is necessary that those employed or contracted to the Group show respect for their colleagues and the work they undertake, and to understand the need for privacy and confidentiality.

8.2.2 All employee's and others with access to email must take the same care in drafting an email as they would for any other communication. All employees are expected to ask themselves, "does this person/persons need to see the contents of this email?" Particular care should be taken with blind copying other recipients and forwarding emails:

8.2.3 Individuals should not forward a message or copy a message or attachment containing personal/sensitive information, belonging to another user without permission from the originator first.

8.2.4 If an Individual is blind copying other persons into an email which is potentially defamatory or confidential they run a risk of being held liable.

8.3 Need to Know

8.3.1 Sensitive information should only be requested on a 'need to know' basis, where the information is necessary to provide a service and only in the best interests of services users or employees.

8.4 Informed and Explicit Consent

8.4.1 Information which is confidential and restricted must only be passed on where there is a clear need to know and where the informed and explicit consent has been obtained from the person whose information needs to be passed on and recorded appropriately.

8.4.2 Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person. Wherever possible, consent should be in writing from the person concerned.

8.4.3 Confidential information should not be discussed on the telephone unless the identity of the caller is established. Where necessary this may need to be checked.

8.5 Circumstances in which Information can be disclosed:

8.5.1 With written consent for a particular purpose.

8.5.2 The information is required by law.

8.5.3 In matters of Child Protection.

8.5.4 Where disclosure can be justified for another purpose and in significant public interest. For example, the protection of the public or the prevention and detection of serious crime.

8.5.5 Difficult decisions should be discussed with a Line Manager or their delegate. They may seek legal advice.

8.5.6 The above is not an exhaustive list. It is crucial that the decision to give sensitive information is a Company decision having followed the correct processes (not the decision of an individual, who

has not followed the correct processes). Should you breach or become aware of a breach please contact the Group Data Protection Officer (DPO) via email at data.protection@ofgl.co.uk

8.6 Storage of Information

8.6.1 Information should be securely and appropriately stored.

8.6.2 Extra care should be taken when working at home or remotely.

8.6.3 Personal Data should only be kept for as long as it is needed

9.0 BREACHES IN CONFIDENTIALITY

9.1 Breaches can happen when sensitive information is given to people who are not authorised to access it.

9.2 Additionally they can happen when procedures are not clear, have not been agreed and have not been followed. Or when information is passed through sections and departments, or when information is in the process of being stored.

9.3 Research indicates that most improper disclosures of confidential information are unintentional.

9.4 Once confidentiality has been broken it may have serious and damaging implications for the Group and its reputation:

A) Specific and Personal information about an individual: If used inappropriately this can cause discrimination, harassment, harmful actions and inappropriate decisions by others.

B) Sensitive Organisation Information: Can be used to damage the Group or other organisations, can threaten progress, security and systems.

9.5 Any breach of confidentiality by employee's such as the unauthorised disclosure to a third party of confidential information about matters connected with the business of the Group will be treated as gross misconduct and could justify dismissal.

9.6 Furthermore, the Group may bring civil proceedings to restrain a member of employee's or contractor or contract service provider from disclosing and /or using such confidential information and claim damages to compensate the company for any loss or expense incurred resulting from a breach of the duty of confidentiality.

10.0 TRAINING AND PUBLICITY

10.1 Guidance on the use and understanding of the Confidentiality Policy and full information is provided as part of the Data Protection Training and within supervision and ongoing employee's training.

11.0 LINKING DOCUMENTS

11.1 This Policy should be read carefully, alongside the following:

- Employment Contract
- Disciplinary Procedures
- Grievance Procedures
- Whistle Blowing Policy
- Data Protection Policy
- Security Policy for Dealing with DBS Information (England and Wales), Access
- Professional Code of Conduct

Outcomes
First Group