

# Data Protection and Information Management Policy

THE LEADER GROUP



## **Policy**

**1.1** The Leader Group recognises that we have a duty of confidentiality to our Clients, Clients / Candidates / Service Users and staff. We believe that respecting an individual's right to a private life, which includes confidentiality, is important in ensuring a trusting, caring environment where both Clients / Candidates / Service Users and staff are confident that information about them will be protected safely and not shared inappropriately or unnecessarily.

It is the policy of The Leader Group that we will only share information that is in the best interest of our Clients / Candidates / Service Users and with their consent. We aim to comply with the relevant legislation and include the [8 Caldicott Principles](#).

### **1.2 Core Principles of Confidentiality**

- All staff will ensure that all Clients / Candidates / Service User information remains confidential. Clients / Candidates / Service Users have the right to expect that personal information held about them is not accessed, used or disclosed improperly
- The same duty of confidentiality applies to personal information about staff, with the exception of names and job titles. Information about Directors, which is published and therefore is a matter of public record, is also excepted.
- All staff have the individual responsibility for ensuring that they conform to the Caldicott principles, Data Protection Act (DPA) 2018 and Article 8 Human Rights Act (HRA) 1998.
- Staff must not inappropriately access, misuse or share any information or allow others to do so. Staff are personally liable for deliberate or reckless breaches of the DPA 2018 and may be liable to disciplinary action and/or prosecution.
- Any personal information given or received in confidence for one purpose may not generally be used for a different purpose, or passed to anyone else without the consent of the provider of the information.

### **1.3 The Position of The Leader Group on Confidentiality**

- We will share with Clients / Candidates, as far as the law allows, the information they want or need to know about their health, care and ongoing treatment sensitively and in a way they can understand
- Confidential information will not be used for a different purpose or passed on to anyone else without the consent of the information provider
- There may be occasions when it can be detrimental to the Clients / Candidates or to another individual if this principle is strictly adhered to
- There is a recognition that breaches of confidence are often unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or

by poor computer security. However, the consequences can be equally serious for all concerned

- The Leader Group will ensure that personally identifiable information will always be held securely and, when used, treated with respect. This rule will apply regardless of where the information is held
- We respect that a person's right to privacy and confidentiality continues after they have died
- All information regarding the Clients / Candidates we work with, will be treated with respect and integrity
- We will be transparent in our approach to ensure that anyone associated with The Leader Group (whether Clients / Candidates) is fully aware of how, what, when, who and why we share any information about them and source their agreement before doing so
- 

**1.4** All relevant staff will be bound by their professional code of practice.

**1.5** All staff must sign a confidentiality agreement as part of their contract of employment (a template can be found within the forms section of this policy). The confidentiality agreement also extends to agency and contract workers.

#### **1.6 Responsibilities – Managing Director**

- Ensuring that systems and processes are in place for the security of records and they are reviewed to ensure that they remain fit for purpose
- Ensuring that all staff understand this policy at the start of employment and that its importance is reiterated during supervision or team meetings
- Ensuring that staff have received the appropriate training and are competent in their role
- Reviewing, monitoring and auditing practice within The Leader Group to ensure that staff remain knowledgeable
- Acting on any breaches in confidentiality in a timely manner and notifying the appropriate bodies
- Ensuring that confidentiality rules are never used as a barrier to sharing appropriate information and fulfilling Duty of Candour obligations

#### **1.7 Responsibilities - All staff will ensure the following:**

- All information that is received is effectively protected against improper disclosure when it is received, stored, transmitted and disposed of
- Confidential information is only accessed if it is appropriate to the job being undertaken
- Every effort is made to ensure that Clients / Candidates understand how information about them will be used before they supply any confidential information

- When Clients / Candidates give consent to disclosure of information about them, they understand what will be disclosed, the reasons for disclosure and the likely consequence/s
- Clients / Candidates understand when information about them is likely to be disclosed to others and that they have the opportunity to withhold their permission
- If disclosing information outside the team that may have personal consequences for Clients / Candidates, that consent is obtained from the Clients / Candidates.
- If the Clients / Candidates withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:
  - They can be justified in the public interest (usually where disclosure is essential to protect the Clients / Candidates or someone else from the risk of significant harm)
  - They are required by law or by order of a court
  - If required to disclose confidential information, staff will only release as much information as is necessary for the purpose
  - The person(s) to whom information is disclosed understands that it is given to them in confidence which they must respect
- When disclosing confidential information, staff must be prepared to explain and justify the decision. Where there are doubts, they will discuss them with The Managing Director
- Queries concerning this policy will be brought to the attention of The Managing Director
- During the induction period for new staff, they will be made aware of this policy and their individual responsibilities

## **Procedure**

**2.1** The Leader Group will detail with transparency how confidentiality is managed with Clients / Candidates, employees and others at the earliest opportunity and seek their agreement, e.g. through existing systems such as recruitment and the pre-assessment process.

Staff can refer to the Fair Processing Notice Templates and the Fair Processing Notice Policy and Procedure for further information that details how information is processed within The Leader Group.

## **2.2 Sharing Information with Other Professionals**

Information sharing between partners, is essential to good practice.

Consent from the Clients / Candidates for information sharing must be recorded following a discussion with the Clients / Candidates or, in the absence of capacity to consent, their designated other.

The principles of sharing information are:

- Only information that needs to be shared
- Only with those who have a clear need to know
- There is a lawful basis for sharing information

### **2.3 General Principles of Confidentiality - Staff will:**

- Understand and follow the Caldicott Principles as detailed within the Forms section of this policy
- Be aware that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared and will seek their agreement unless it is unsafe or inappropriate to do so
- Seek advice from The Managing Director, if they are in any doubt, without disclosing the identity of the person, where possible
- Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Staff may still share information without consent if, in their judgment, that lack of consent can be overridden in the public interest
- Consider safety and wellbeing: Staff must base information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information shared is necessary for the purpose for which it is being shared, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely
- Staff must keep a record of any decision and the reasons for it (to include what has been shared, with whom and for what purpose), and for the decision not to share

### **2.4 Maintaining Confidentiality**

- All information we hold will be treated with respect and integrity
- In general, no information may be disclosed either verbally or in writing to other persons without the Clients' / Candidates' consent.
- If in doubt, you can consult the Line Manager or The Managing Director
- Conversations relating to confidential matters affecting Clients / Candidates must not take place anywhere they may be overheard by others, i.e. in public places - such as supermarkets, public transport, open plan areas of the office or during training events.
- Written records and correspondence must be kept securely at all times when not being used by a member of staff. Confidential information must not be left in an unattended vehicle
- Staff must not disclose any information that is confidential or that, if it were made public, may lead to a breakdown in the trust and confidence that the Clients / Candidates have in The Leader Group

- Staff must not pass on any information or make comment to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries

## **2.5 Safeguarding, The Care Act and Confidentiality**

Where safeguarding issues arise and in order to fully understand what has gone wrong, LADO / Safeguarding Adult Boards may ask for information to be shared. Decisions about who needs to know and what needs to be known should be taken on a case-by-case basis, within locally agreed policies and the constraints of the legal framework. However:

- Staff must verify the identity of the person requesting the information whilst establishing if it can be anonymised (refer to 5.8)
- Information will only be shared on a 'need to know' basis when it is in the interests of the child / adult
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained, but if this is not possible and other people are at risk of abuse or neglect, it may be necessary to override the requirement
- It is inappropriate for The Leader Group to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when others may be at risk

## **2.6 Rights of All Clients / Candidates**

All Clients / Candidates may view personal information we hold about them. Local and health authorities are not required to give access to information that is 'hurtful' or 'that would breach the confidentiality of another Clients / Candidates. The policy at The Leader Group is to record information in a way that, as far as possible, avoids a need for this exclusion. If a Clients / Candidate believes their right to confidentiality is either being breached or undermined, they must have access to the complaints procedure at The Leader Group.

Staff must refer to the Subject Access Requests Policy and Procedure for further details.

## **2.7 Rights of All Staff**

All staff may view personal information held by The Leader Group that relates to them, by applying in writing to their Line Manager or Registered Manager, The Managing Director.

## **2.8 Data Security and Quality**

- Any record that contains information about an individual must remain confidential unless it is in the public domain. Any records will be factual and will not include the personal opinions of the person writing the records.
- Reproduction of information relating to a Clients / Candidates (e.g. photocopying documents) will only be done with the consent of the Clients / Candidates
- Confidential information to be posted must be marked 'Private & Confidential, for attention of the addressee only', and sent recorded/special delivery

Staff can refer to the guidance contained in the Forms section of this policy for best practice and requirements for data security. However, as a minimum:

- Information held within The Leader Group will not be shown to unauthorised individuals or be left where authorised personnel may access them. All records will be kept in a lockable cabinet in a lockable office, with restricted access
- All written records will be kept securely and only disposed of by shredding, after appropriate timescales. Staff must take care when recording personal identifiable information into personal notebooks or paper during shift handover and ensure the safekeeping and destruction of the information
- Any employee who breaches this policy may be subject to disciplinary procedures

## **2.9 Social Media**

Staff are not permitted to discuss clients, students or other employees past or present, or The Leader Group on any social networking site, as this may breach confidentiality and bring The Leader Group into disrepute. Staff must also be aware that this applies to taking and posting photographs of Clients / Students / Candidates.

## **2.10 Anonymisation and Pseudonymisation Considerations Anonymisation**

Anonymised information (i.e. where personal information is removed and both the giver and the receiver are unable to identify the Clients / Candidates) is not confidential and may be used outside of data protection legislation. However, staff should be aware that information which contains small numbers of person identifiable information may lead to identification. For this reason, all disclosure of anonymised information must be reviewed on a case-by-case basis. The Leader Group will seek to anonymise collective data about individuals within the service.

### **Pseudonymisation**

Pseudonymisation is the practice of removing and replacing actual data with a coded reference (a 'key'). The Leader Group will consider this practice where the use of the data needs to relate to individual records, but also needs to retain security and privacy for that individual. There is a higher privacy risk and security risk of the key system as the data will not truly be anonymised.

Personal data that has been pseudonymised can fall within the scope of data protection legislation, depending on how difficult it is to assign it to a particular individual.

Further information can be found within the ICO [Anonymisation Code of Practice](#).

### **2.11 The Leader Group Confidentiality Suppliers**

Staff must extend the principles of confidentiality when considering The Leader Group sensitive information and the protection of any commercial data.

Staff and/or external suppliers will ensure that information such as suppliers' prices, performance and costs are not disclosed to other suppliers or unauthorised persons. The Leader Group could consider requesting that suppliers sign a confidentiality agreement in order to protect the data of The Leader Group.

If there are any queries about how to support commercially sensitive information, these must be discussed with The Managing Director.

### **Meetings**

The Leader Group has a right to have confidential meetings where information is discussed and then held securely and confidentially. Information held will be in line with the Freedom of Information Act (FOIA) 2000 and the Data Protection Act 2018.

### **Complaints and Investigations**

Complaints and investigations are treated confidentially and remain so unless there is a legal requirement to release information.

### **Media**

Staff must not pass on any information, or make comments, to the press or other media. Media enquiries must be referred to the person responsible for handling any media enquiries.

### **2.12 Confidentiality Breach**

Unauthorised access, use or disclosure may be in breach of the DPA 2018, the Human Rights Act, and/or breach the policies of The Leader Group and may lead to disciplinary action.

Where there has been a breach in confidentiality, this will be recorded on an incident form at The Leader Group and reported to The Managing Director.

Significant breaches will be reported to Managing Director so that reporting to the relevant regulatory, professional bodies and the ICO is considered.

Breaches will be monitored by The Managing Director, reflected on with lessons learned and will form part of the quality assurance programme for The Leader Group.

Staff will refer people to the Complaints Policy and Procedure at The Leader Group.