Reference	247 POL 23
Version	1.0
Issue Date	18/01/2022
Approved	MD
Review Date	05/01/2027

247 ALLIANCE LTD

CONFIDENTIALITY POLICY

PURPOSE

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within 247 Alliance Ltd. have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. All employees working in the 247 Alliance Ltd. are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc. of personal data, states it is an offence for a person knowingly or recklessly:
(a) to obtain or disclose personal data without the consent of the controller.
(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

This policy sets out the requirements placed on all staff when sharing information within the 247 Alliance Ltd. and between our clients. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per Encryption Guidance.

Scope

All our staff and of client organizations, without exception, are within the scope of this policy, including and without limitation.

Roles and Responsibilities

Managing Director

The Managing Director has overall responsibility for strategic and operational management, including ensuring that 247 Alliance Ltd. comply with all legal, statutory, and good practice guidance requirements.

Data Protection Officer (DPO)

Data Protection Officer (DPO) to provide advice to the highest level of the organisation and all of its employees on data protection issues which can include confidentiality issues which would be reviewed as appropriate to ensure the organisation's compliance with data protection law.

Manager HR

Manager HR with responsibility for HR is responsible for ensuring that the contracts of all staff are compliant with the requirements of the policy and that confidentiality training is included in inductions for all staff.

Contract Managers

Contract Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated, and acted upon via the Information Security Incident Reporting Procedure.

All staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Data Protection Act 2018 and GDPR. There is a Confidentiality clause in their contract, and it is mandatory to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Keeping and Safeguarding Records

- Records relating to employees and client organization are available to relevant staff/ who have undergone selection and training.
- Care must be taken at all times by employees to ensure that all records are handled with discretion and are secured when the premises are not staffed.
- Correspondence and other records, minutes, files, database appertaining to an individual or organisation should not be left on desks and notes should be destroyed once case files/database records have been compiled.
- Appointment diaries and any other documentation which contains personal information should be left in the office at weekends and holiday periods and stored securely when taken out of the office.
- All paper enquiry records should be kept in lockable cabinets if they cannot be transferred on to database, with access limited to relevant staff.
- Old records and files should be regularly monitored, and information destroyed when it is no longer necessary to keep it. Files, papers, records containing names and addresses should, when no longer needed, be.

Removal of Information from the Premises

- It is sometimes necessary for staff to carry information relating to clients with them on home visits or when attending meetings or case conferences. Staff are expected to exercise due care and attention to ensure that such material is kept to a minimum, is safe and in their possession at all times. Particular care should be taken with diaries and other documentation where appointments indicate the name and address of a service user. No such material/information should be left unattended in a vehicle. Papers should be returned to the office as soon as possible and always before the end of the working day.
- Electronic devices used in community work should be password protected and stored securely. This includes smartphones, tablets, laptops and USB or other external storage devices.

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes, and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended. Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers. Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is

gross misconduct which may result in summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted. Under no circumstances should employees access records about their own family, friends, or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Senior Management Team and relevant Managers and may be subject to external audit. The Managing Director is responsible for the monitoring, revision and updating of this document on a 2 yearly basis or sooner if the need arises.

Malik Mustafa
Director
05/01/2026

Signed 

Review Date: 05/01/2027