



Breakaway

Confidentiality policy

Policy Owner:	Ranbir Sidhu (Registered Manager)
Version:	1:4
Date:	June 2025
Review Date:	June 2026

Policy Summary:

Regulation 12, 13, 38 of the Children's Homes Regulations 2015 including the Quality Standards

CONFIDENTIALITY:

The Aim of the Policy is to;

- Define degree to which sensitive data about both individuals and organisations must be protected.
- Ensure Information is not made available or disclosed to unauthorised individuals, entities or processes.
- Outline the meaning of confidentiality, its importance within the unit, how to maintain and respect it and details on our ways of working with it.
- Virtual meetings/ Office 365

References:

GDPR, Information Governance

Disclosure of Confidential Information

Disclosure of confidential information without the consent of the subject is only permissible in strictly limited and exceptional circumstances, where legal obligations or the public interest may outweigh the subject's right to confidentiality.

Confidential information should only be accessible to those directly involved with the subject, and only to the extent necessary to maintain good practice and standards. This may include, but is not limited to, the following individuals:

- Social Workers
- Management staff
- Senior Management
- Social Carers
- Authorities Finance staff
- Legal staff
- Police
- Department of Health's Social Services Inspectorate
- Guardians
- Independent Reviewing Officer
- NHS

Confidentiality in Telephone Calls

When you answer the telephone and the caller requests information about an individual child, colleague, or family you must first clarify the following:

- Their name
- Organisation/Team
- Contact number

- Nature of query

If an individual makes a request for information, explain that you will gather the necessary details and call them back. This provides an opportunity to verify the caller's identity with colleagues, managers, or social workers and confirm whether they are entitled to the information. Once verified, you can return the call and provide the requested information. If you are unable to fulfill their request, direct them to the appropriate person, such as a manager or social worker.

If someone inquires about the services offered, explain that we are a short breaks unit and refer them to management or Observatory House for further information.

Under no circumstances should you disclose our address or confirm whether a child or staff member is using the service unless the caller's identity has been verified. This policy is in place to ensure the protection of both children and staff.

Confidentiality of Manual Records

Manual records must be securely protected from unauthorized access, modification, or loss due to accidental or deliberate damage, erasure, or disclosure. These records should be stored in locked, secure cabinets to ensure their confidentiality and integrity.

Confidentiality on Computer Systems

Computer systems must be protected against unauthorized access, modification, or loss due to accidental or deliberate damage, erasure, or disclosure. Failure to exercise reasonable care could result in legal action for compensation under Section 13 of the Data Protection Act 1998. Only authorized personnel should have direct access to the record systems, which must include mechanisms to restrict access to information based on necessity, such as password protection.

Confidentiality and Staff

- Staff must not discuss individual children in front of other children's parents or carers.
- Staff must not discuss other staff members in front of children's parents or carers.
- Staff must not discuss children in public. If it is absolutely necessary, only the child's initials should be used.
- Staff should not expect other colleagues to keep information secret if it could impact practice, such as breaking a child's personal belongings.
- Staff must not promise to keep a child's secret, as this may involve a disclosure of important information. It is essential to explain this to the child before any conversation takes place.

Virtual Meetings/ Access to office365

As we continue to adapt to the post-Covid-19 era, attending meetings remotely from home has become the norm. While this offers convenience, it also presents risks to maintaining confidentiality. Staff must adhere to the following guidelines to ensure confidentiality is maintained when attending virtual meetings or accessing Office 365 to check emails:

- Staff must attend meetings from a private location where other household members cannot overhear the discussion.
- Headphones (provided in each office) must be worn during meetings to protect confidentiality.
- Staff are prohibited from downloading personal data of service users onto their personal devices.
- Recording of meetings is not permitted unless prior approval is obtained from the meeting chair.
- Staff should keep their video camera on during meetings, unless otherwise instructed.
- Staff must not join meetings while driving.
- Staff must inform the chair if they need to take a break and should never leave the meeting page unattended.
- Staff must ensure they log out of systems, especially when using shared devices.
- Staff must not share emails or attachments with anyone who is not authorized to view them.
- Secure email (Encrypt) should be used when sending personal data.
- Any breach of confidentiality must be immediately reported to HR and the Information Governance team.