

Policy 7

Confidentiality Policy 2026/2027

The purpose of the Confidentiality Policy is to ensure that all staff, members and users understand the organisations requirements in relation to the disclosure of personal data and confidential information.

7.1 Policy Statement

7.1.1 Reach is committed to providing a confidential service to its users. No information given to Reach will be shared with any other organisation or individual without the user's expressed permission unless in any circumstance where an individual or organisations welfare is at serious risk of harm, neglect and danger.

7.1.2 For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the organisation through its work.

7.1.3 Reach holds personal data about its staff, users, members etc. which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission.

7.1.4 All personal data will be dealt with sensitively and in the strictest confidence internally and externally. All information on students/young people is passed on and shared with the commissioning school/body regularly including weekly reports, email updates and relevant meetings attended.

7.2 Principles

7.2.1 All personal paper-based and electronic data must be stored in accordance with GDPR (General Data Protection Regulation 2018) and must be secured against unauthorised access, accidental disclosure, loss or destruction.

7.2.2 A password must be used on work phones and laptops. Ensure password credentials are not saved for any shared use device. 2FA (2 Factor Authentication) will also be used for programmes used where available.

7.2.3 Staff partners, families and children must not have access to any Reach portals or information.

7.2.4 No confidential information on any student (other than the youth club young people) is permitted to be stored at the Reach base.

7.2.5 All personal paper-based and electronic data must only be accessible to those individuals authorised to have access.

7.2.6 Staff must ensure that no students have any access to any confidential information on other Reach students.

7.2.7 All email and text communications must only include the initials for students/young people which are referenced and not their full names. This includes all report writing and other forms of correspondence.

7.2.8 Staff must not discuss names of students/young people with whom they are working with to their partners/family members or the wider networks outside of Reach staff team and contracted partnerships/agencies.

7.3 Statistical Recording

7.3.1 Reach is committed to effective statistical recording of the use of its services to monitor usage and performance.

7.3.2 All statistical records given to third parties, such as to support funding applications or monitoring reports for the local authority shall be produced in anonymous form, so individuals cannot be recognised.

7.4 Breaches of Confidentiality

7.4.1 Reach recognises that occasions may arise where individual workers feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged where there is risk of danger to the individual, a volunteer or employee, or the public at large, or where it is against the law to withhold it. In these circumstances, information may be divulged to external agencies e.g. police or social services on a need to know basis. This includes for safeguarding purposes and multi-agency working (all information).

7.4.2 Where a worker feels confidentiality should be breached the following steps will be taken:

- The worker should raise the matter immediately with Duty.
- The worker must discuss with Duty the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The Director should take a written note of this discussion.
- Duty is responsible for discussing with the worker what options are available in each set of circumstances.
- The Director (or DSL) is responsible for deciding on whether confidentiality should be breached. If the Director (or DSL) decides that confidentiality is to be breached, then a plan will be made to move forward and do so.

7.5 Legislative Framework

7.5.1 Reach will monitor this policy to ensure it meets statutory and legal requirements including the Data Protection Act, GDPR, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training on the policy will include these aspects.

7.6 Ensuring the Effectiveness of the Policy

7.6.1 All staff members will receive a copy of the confidentiality policy. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually, and amendments will be proposed and agreed by the Director. Copies of privacy notices must also be studied. The data controller for Reach is the Director.

7.7 Non-adherence

7.7.1 Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.

Any further questions regarding guidelines in this policy then please contact one of the leadership team.

To ensure the effectiveness of this document our 'Confidentiality' policy will be reviewed annually.

Signed:



Date: 2nd Sept 2026

Dan Palmer

Founder / Director