

Merton Mencap

Confidentiality Policy

Last reviewed
February 2026

Next review
February 2028

**This policy and procedure has been adopted by Merton Mencap
through its Executive Committee which remains responsible for its review**

Merton Mencap

Confidentiality Policy

Introduction

Merton Mencap takes its responsibility in relation to confidentiality very seriously. This policy applies to all staff, ie employees and volunteers.

Our Data Protection Policy and Privacy Notices explain how we manage confidential information. This Policy sets out our general expectations for staff.

Personal information

Merton Mencap will provide all staff with training in confidentiality/General Data Protection Principles (GDPR), i.e. this is mandatory, reviewed every 2 years.

Our 'Privacy Notice for Service Users' explains how we collect and use information about people with learning disabilities/autism and parents and carers who use our services (ie service users)

Our 'Privacy Notice for Applicants, Employees and Volunteers' and 'Privacy Notice for Supporters' explains how we collect and use information about these individuals.

Our 'Privacy Notice for Supporters' explains how we collect and use information about them.

We will store Personal Information in a secure system, either on our password protected IT system or in a lockable filing cabinet at our office. If hard-copy Personal Information must be taken out of our office, we will conduct a risk assessment beforehand to ensure its safety. Portable storage devices (e.g. USB sticks) are not permitted to be used.

When accessing documents (eg computer or paper record) or having conversations which contain personal information staff must ensure against information being viewed by others.

Staff should avoid talking about individuals in social settings and exchanging personal information or comments (gossip) about others with whom they have a professional relationship. Staff *are* able to share information with their line manager in order to discuss issues and seek advice.

External parties

It may be necessary to share confidential information with third parties, eg HR and pension providers.

Contracts covering this work will specify the confidential nature of the work and will reflect this policy, our Data Protection Policy and Privacy Notices.

Duty to disclose

Merton Mencap recognises its duty to disclose information such as suspected abuse, drug trafficking, money laundering, acts of terrorism or treason to the relevant authorities.

We recognise our duty to refer current/previous staff to the Disclosure and Barring Service, eg if the individual has been dismissed as a result of an illegal act.

If a member of staff believes an illegal act has taken place, or that an individual is at risk of harming themselves or others, they must report this to their line manager who will report it to the appropriate authorities. They should also refer to our Whistleblowing policy.

If during supervision a serious disciplinary issue comes to light, it may be necessary to disclose this information and proceed in accordance with our Disciplinary and Grievance procedure. The person concerned should be informed of any disclosure.

Breach of confidentiality

Staff accessing unauthorised files or breaching confidentiality may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

Whistleblowing

Merton Mencap recognises the rights of staff not to suffer detriment or be unfairly dismissed as the result of speaking out about crime, fraud, miscarriages of justice, dangers to health and safety, breaches of civil service code or risks to the environment.

See the whistleblowing policy for more information.
