

Little Miracles
The Spinney,
Hartwell Way,
Peterborough,
Cambridgeshire,
PE3 7LE

Registered Charity: 1160178



Confidentiality and Data Protection & Security 2026

Date of last review: 4th January 2026

Date of next review: 3rd January 2027

Signed (Chair, Little Miracles)

Little Miracles is bound by the UK's Data Protection Act 2018. This protects personal data and restricts an organisation's ability to disclose personal data. Personal data is information relating to an individual from which they can be identified, e.g. name, address, tax details or national insurance number.

Little Miracles staff and volunteers may be given personal information in confidence by an individual service user or group of service users. Anyone working for Little Miracles has a duty to protect the confidentiality of personal information and to process personal information with the correct safeguards.

Little Miracles Data Protection Officer is Michelle King.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Data protection principles, means the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Information can be requested for the following reasons;

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

Data Controller Status

As Little Miracles retains personal information for the organisation's use, we follow our legal duty to register with the Information Commissioner's Office as a Data Controller.

Handling complaints

If a member of the public is concerned about their information rights practices, Little Miracles is responsible for dealing with the matter.

Little Miracles will respond to any information rights concerns received, clarifying how we processed the individual's personal information in that case and explaining how we will put right anything that's gone wrong.

If a member of the public has engaged with Little Miracles but is still dissatisfied, they may report their concern to the Information Commissioner's Office.

Requests for Access to Data Held

If an individual wishes to see any personal information about them held by Little Miracles, this can be shown to him or her and a copy made if one is requested.

They are entitled to see:

- a description of the personal data;
- the purposes for which they are being processed;
- and the discloses, or potential discloses, of the personal data.

To ensure that the request is a genuine one, a request email or form should be sent to the person to complete. If a third party is acting on behalf of the individual, proof of the third party's identity and the individual's authority to disclose their information to their representative, must be obtained in writing. All requests must be responded to within 20 working days.

Confidentiality and telephone support

Little Miracles telephone support is bound by this confidentiality policy.

The following statement about confidentiality will be stated by the Telephone Support Worker during the course of each telephone call:

"The information you give me will be dealt with confidentially. However if you want family assistance, we will need your agreement to pass some of your personal details to organisations that may be able to help you."

Any email support service should include a line under the signature

"Little Miracles support services are confidential and secure. However if you want external family assistance, we will need your agreement to pass some of your personal details to organisations that may be able to help you."

Many of the calls that Little Miracles advisers handle will involve discussion of callers' personal information and circumstances, in particular health and financial matters.

When undertaking these services on behalf of callers, telephone advisers should remind callers of the confidential nature of the service and that their agreement to the sharing of this information may be needed in order to apply for additional support or grants on their behalf. It should be made clear to the caller which organisation the information will be sent to. Callers should also be sent a copy of any letters, forms, emails or other communications containing their personal information that have been sent to organisations.

There are certain other circumstances in which confidentiality may need to be broken. These are outlined in this policy under 'breaking confidentiality' together with the procedures that Support Workers should follow.

Data Protection – Security

Little Miracles commits to take the following security measures to protect data in its care:

- Install a firewall and virus-checking on Little Miracles computers.
- Set the operating system up to receive automatic updates.
- Protect Little Miracles computers by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow Little Miracles staff and volunteers access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on Little Miracles computer systems and keep them in a separate place.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Install an anti-spyware tool.
- Consider whether the content of email should be encrypted or password protected.
- Be sure emails are sent to the right addresses.
- Use blind carbon copy (bcc) on group email to protect the recipients from obtaining others email addresses.
- Check that the recipient's arrangements are secure before sending email messages.
- Consider whether secure email or courier may be more secure than fax. Only fax

information that is required.

- Double check fax numbers. It is best to dial from a directory of previously verified numbers.
- Check that sending a fax to a recipient with adequate security in place.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.
- Shred all confidential paper waste.
- Check the physical security of our premises.
- Train staff and volunteers so they know what is expected of them;
 - to be wary of people who may try to trick them into giving out personal details
 - so that they know they can be prosecuted if they deliberately give out personal details without permission;
 - to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
 - not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
 - not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
 - not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Breaking Confidentiality

Confidentiality may be broken in the following circumstances:

- Where the person from whom the information was obtained, and (if different) the person to whom it relates, consents
- Where the information is already available to the public from other sources
- Where the information is in the form of a summary or collection of information so framed that it is not possible to ascertain from it information relating to any particular person

- When there is a serious risk of harm to the individual, as in a threatened suicide
- To protect others. For example, information about possible child abuse should be disclosed to the appropriate agency. See the Little Miracles Safeguarding Policy.
- To prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.

Information about a Crime

It is a criminal offence to:

- Deliberately mislead the police
- Receive a reward of any kind in return for not notifying the police about a criminal act
- Fail to notify the police about an act that could be construed as an act of terrorism
- Fail to notify the police about an act that could be construed as drug trafficking
- Knowingly take monies from a benefits agency fraudulently.

If a member of Little Miracles staff has to break confidentiality, or consider breaking it, then the person whose personal information it is must be told that this is going to happen, verbally if possible, or in writing if suitable. The member of staff should only do so after all attempts to persuade the individual to disclose the information voluntarily have failed. The Little Miracles Manager should be consulted before disclosure. They will make the final decision about breaching confidentiality.

Data Sharing

In order to provide the most effective support package for service users, there may be times when it is necessary to share users' personal information with other organisations. Any requests for information made to Little Miracles through an organisation will be obtained in writing and data will only be provided once the service user has consented to the data being collected and in accordance with the organisation's own Data Protection, confidentiality and privacy policies.

Publication

The fact that Little Miracles services, are confidential and secure will be stated in all social media, websites, email and other publicity and information materials. Little Miracles will display it's charity number on all publications and accurately use the logos of their funders in consultation with these funders.

Disclosure and Barring Service

Data received through seeing staff and volunteers' Disclosure and Barring Service Checks will be stored, handled and secured appropriately in line with the Disclosure and Barring Service Code of Conduct.

Training

Little Miracles will induct employees and volunteers in the importance of data protection and confidentiality, maintain ongoing reminders raise awareness of the issue in its premises.

Subject Access Request Policy.

Introduction Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Our business must comply with the requirements of the General Data Protection Regulations (GDPR) and we must be able to demonstrate compliance to the Information Commissioner's Office (ICO). Upon receipt of a request for information our policy is as follows: Responsibility Michelle King is responsible for the handling of Subject Access Requests (SAR) in our business. The duties of the include but are not limited to:

- Log the receipt and fulfilment of all requests received from a data subject/the person making the request/ requestor to see his or her personal information.
- Acknowledge the subject access request (SAR).
- Verify the identity of any person making a SAR.
- Maintain a database on the volume of requests and compliance against the statutory timescale.
- Verify whether if we are the controller of the data subject's personal data.
- Check if we are not a controller, but rather a processor. If so, inform the data subject and refer them to the actual controller. This needs to be recorded in writing.
- Where applicable, decide if a request is excessive, unfounded or repetitive and communicate this to the requestor.
- Decide if an exemption applies.
- If a SAR is submitted in electronic form, any information should preferably be provided by electronic means as well.

Oral or written requests Subject access requests can be made in writing, electronically or verbally.

Making a request

- If an employee wishes to make a subject access request to verify the lawfulness and accuracy of the personal data we hold about them, they are encouraged to submit their request to the Data Controller in writing (letter or e-mail).
- The request should be specific about the nature and the type of data required.
- Every attempt will be made to comply with the request in a timely manner and without undue delay.
- Upon receipt of the information the employee is encouraged to check the accuracy of the information and to advise the Company of any updates that may need to be made.

- A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.