

M13 YOUTH PROJECT Data Protection Policy Updated May 2018

The Data Protection Act 2018 (c.12)¹ ("The Act") (which includes the General Data Protection Regulation "GDPR") is designed to protect the rights and privacy of individuals and to ensure that data about them is processed using the appropriate lawful basis and in appropriate ways.

M13 Youth Project ("M13") takes seriously its obligations under the Act and the purpose of this policy is to enable M13 to comply with the law in relation to data it holds about individuals.

1 Scope of the policy

The Act applies to **personal data**, meaning any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It also applies to sensitive personal data, meaning personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. The Act applies to both automated personal data and to manual filing systems where personal data is accessible.

M13 collects the following personal data every year including:

- Staff records ("staff" includes paid employees, workers and volunteers);
- Names, addresses, dates of birth, gender, ethnicity, religion, medical information, parental and second/emergency contact information, photographs of and recordings of meetings with young people with whom we work; and
- Names and addresses of supporters and members.

2 Responsibilities and Confidentiality

- 2.1 The Trustees of M13 recognise their responsibility in ensuring that M13 complies with its legal obligations. M13 is the Data Controller under the Act. The Manager of M13, Helen Gatenby, has overall responsibility for this policy.
- 2.2 All staff are required to read and accept this policy and are responsible for ensuring their compliance with this Policy. Significant breaches of this policy will be dealt with under M13's disciplinary procedures. Misuse of personal data is a disciplinary offence and may even constitute a criminal offence.
- 2.3 In addition to this policy, all staff should refer to the *M13 Youth Project Ethical Guidelines on Collection and Handling of Young People's Data*.

¹ The Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf date accessed 16 May 2018

- 2.4 When working for M13, staff will often need to have access to personal data which may include, for example, personal information about young people, supporters or those involved in activities organised by M13; information about the internal business of M13; and personal information about colleagues working for M13.
- 2.5 M13 is committed to keeping this information confidential, in order to protect the individuals concerned and M13 itself. "Confidential" means that all access to such information must be on a need to know and properly authorised basis. Staff must only use the information they have been authorised to use and for the purposes that have been authorised. Staff should also be aware that under the Act and GDPR, unauthorised access to data about individuals is a criminal offence.
- 2.6 Staff must be particularly careful not to disclose information to unauthorised people or cause a breach of security. In particular they must not compromise or seek to evade security measures (including computer passwords), not talk about confidential information with people outside M13 and not disclose information, especially over the telephone, unless they are sure that they know to whom they are disclosing it and that the person to whom they are disclosing information is authorised to have it. If staff are in any doubt about whether to disclose information or not, they should withhold the information while they check with the M13 Manager.
- 2.7 Staff's confidentiality obligations continue to apply indefinitely after they have stopped working for M13.

3 Staff Data

- 3.1 Various data is held on staff relating to their employment/volunteering with M13. This will cover all aspects of recruitment, selection and employment such as the job / volunteer application form, interview assessments, references, probationary and annual reviews and supervisions, bank details and national insurance number, details of any deductions from pay, sick notes and medical assessments, details of grievance and disciplinary proceedings, reference requests etc. Much of this data is, by its nature, highly personal and M13 recognises its duty to safeguard the data by appropriate means, and to notify staff about what is kept and why, along with information on how the data can be accessed and by whom.
- 3.2 The data kept on staff is exclusively in relation to their employment/volunteering with M13; no unrelated data will be kept. The data that is kept will be used for the purpose of administering and managing their work with the project.
- 3.3 Most personal data is kept in individual personnel files in the M13 office and these are locked. Other data (e.g. bank details, NI number, payroll details) is kept by the Administrator in computer files that are password protected. Payslips and paperwork relating to employees are kept in a file in a locked filing cabinet in the office.
- 3.4 All staff contracts/working agreements include information on data protection, and make clear that by signing the contract/agreements, staff give consent for M13 to keep the data outlined above and to use it in the ways outlined above. Access to staff data is restricted to Management at the appropriate level and to administrative staff for any issues specifically relating to pay, file maintenance, employment correspondence and the like. Staff are entitled to see their own personnel files. To do so, they should arrange a mutually convenient time with the Manager.

- 3.5 Data relating to staff will be kept for 7 years following the termination of their employment with M13.

4 Young People's Data

- 4.1 M13 recognises its duty to safeguard the data it holds on young people. To this end at regular intervals M13 conducts an audit of data held, disposes of outdated information and arranges secure storage systems for current data including locked and password protected storage and locked archive facilities.
- 4.2 All staff should refer to the *M13 Youth Project Ethical Guidelines on Collection and Handling of Young People's Data* for information on the collection, storage and use of young person's data.

5 Members' and Supporters' Data

- 5.1 M13 recognises its duty to safeguard the data it holds on its members and supporters. To this end at regular intervals M13 conducts an audit of data held, disposes of outdated information and arranges secure storage systems for current data including locked/ password protected storage and locked archive facilities. In addition, members and supporters are informed that their personal data will be held by M13 for the purpose only of corresponding with them.

6 People's Request to Access their Data (Subject Access Request)

- 6.1 Any M13 staff member, young person with whom M13 works or M13 supporter is entitled to know what data is kept on her/him, why, how it is kept, and who can access it. They may see what data is kept on them and correct it if necessary.
- 6.2 Any requests for access to data should be made in writing to the M13 Manager. All staff and volunteers are required to pass on anything which might be an access request to the M13 Manager without delay. Where the individual making an access request is not personally known to the M13 Manager, their identity will be verified before any information is released. All requests will be dealt with within one calendar month of receipt, as required under the Act. In response to a valid request, M13 will provide a permanent, intelligible copy of all the personal data relating to the Data Subject held at the time of the request. No charge will be made for access.
- 6.3 Where the person making a Subject Access Request would like support to submit that request in writing, M13 staff shall offer support to enable them to do so.

This policy was adopted by M13 Youth Project Trustees in June 2018 and is reviewed annually in June.