THE MATTHEW PROJECT
Finding hope together

E-Safety Policy

This is a non-contractual policy

Created: November 2023
Review date: November 2025
Approved by CEO & Board Trustees

E-safety is a term that refers to the protection of users from online risks, such as cyberbullying, grooming, hacking, phishing, identity theft, and exposure to inappropriate or harmful content.

E-safety also involves educating users about how to behave responsibly and respectfully on the internet, and how to report any concerns or issues they may encounter.

E-safety is important for everyone who uses the internet, but especially for children and young people who may be more vulnerable or unaware of the potential dangers.

E-safety risks can be grouped into four categories:

- Conduct: people's behaviour may put them at risk, such as sharing personal information, posting inappropriate comments, or engaging in illegal activities.
- Content: access to inappropriate or unreliable content may put people at risk, such as violent, sexual, extremist, or misleading information.
- Contact: interaction with unsuitable, unpleasant, or dangerous people may put people at risk, such as strangers, bullies, predators, or scammers.
- Commercialism: people's use of platforms with hidden costs may put them at risk, such as online games, apps, or websites that require payment or personal data.

Policy Aims

The purpose of the E-Safety Policy (the "Policy") is to:

- Ensure the safety and wellbeing of our staff, volunteers ("Workers"), service users, and anyone involved in The Matthew Project's activities whilst they are using the internet, social media, or mobile devices.
- Provide Workers with the overarching principles that guide The Matthew Project's ("TMP") approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Policy Scope

The Policy applies to all Workers, service users, and anyone involved in TMP's activities, and it reflects the safeguarding needs of the children, young people, and vulnerable adults who our organisation works with. It should be read alongside other relevant policies and procedures.

Our Policy

<u>We believe that:</u>

- Children, young people, and vulnerable adults should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.

<u>We recognise that:</u>

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- We have a duty to ensure that all children, young people, and vulnerable adults involved in our organisation are protected from potential harm online.
- We can help support keeping our service users safe online, regardless of whether they are using TMP's network and devices or not.
- All service users, regardless of age, disability, gender reassignment, race, religion/belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, young people, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

<u>We will seek to keep service users safe by:</u>

- Appointing an E-Safety Coordinator (our Safeguarding Lead).
- Providing clear and specific directions to Workers on how to behave online through our Code of Conduct Policy and Working with Clients Online Safeguarding Policy.
- Supporting and encouraging our service users to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that usernames, logins, email accounts and passwords are used effectively.
- Ensuring personal information about service users is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only with their consent, and only for the purpose for which consent has been given.
- Providing support and training for workers about online safety.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.
- Actively discouraging children and young people to register for apps, software or platforms which are not age appropriate.

<u>We will respond to online abuse by:</u>

- Having clear and robust safeguarding procedures in place for responding to abuse.
- Providing support and training for Workers on how to deal with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse, and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders, and our organisation into account.
- Developing a plan to address online abuse and review it regularly to ensure that any problems are resolved in the long term.

E-Safety Training and Information

Workers and service users will be informed about key risks by posters which are easily visible wherever computers are used on Matthew Project premises.

Data providers and other agencies collaborate to safeguard Workers and service users in accordance with current government guidance.

No service user is to use any Matthew Project computer or other IT equipment without a Worker present at all times. This practice not only provides immediate support where required, but also a general oversight of computer use.

Workers will undertake core mandatory initial training in E-Safety, and General Data Protection Regulations. This training may be through e-learning, or face to face training, or a blended method. Following initial training, all Workers will update E-Safety training every two years.

Training of Workers will be monitored by the E-Safety Coordinator.

Workers and service users with learning difficulties and/or other disabilities should be offered an individualised learning programme which meets their needs.

Monitoring Software

The Matthew Project service provider will ensure that all computers on which service users or visitors have access, are enabled for ‘Parental Guidance’.

Parental Guidance software monitors the inappropriate use of language and blocks certain websites where content may be offensive or illegal.

The E-Safety Coordinator must maintain regular scrutiny to ensure the Parental Guidance is never turned off.

The Matthew Project works with its service provider to provide a system where internet usage can be monitored by the E-Safety Coordinator.

All service users and visitors will be required to accept the terms of an Acceptable Use of ICT Policy before logging on to a Matthew Project computer for internet use.

The Matthew Project will maintain a separate Internet Access/Wi-fi system for use by service users or visitors so that there is no congruence between the internal Workers’ systems and that used by service users or visitors.

The Matthew Project will work with its provider to ascertain whether a similar Parental Guidance software can be put onto the service user and visitor access system.

The Matthew Project internet systems will be reviewed regularly, including anti-virus and firewall software.

Continuous Education and Learning

The Matthew Project will comply with copyright legislation where internet materials are used by Workers, service users and visitors.

The importance of cross-checking information before accepting its accuracy will be discussed with each new user.

Information on how to identify unpleasant, inappropriate, or illegal internet content will be displayed, and discussed with each new user. All users will be asked to report any such content to the E-Safety Coordinator.

The E-Safety Coordinator will monitor the content reporting systems.

General E-Safety Guidance

Incoming electronic communications should be treated as suspicious, and attachments never opened unless the author is known, and content expected.

Internet users should not arrange to meet anyone met only through internet contact.

Internet use will be monitored according to the Matthew Project's Safeguarding Policy.

Workers will receive training and updates on helping service users to use social media platforms appropriately.

The Acceptable Use Policy will request permission for the Matthew Project to monitor where social media platforms are being used on Matthew Project computers.