

MAP Online Safety Policy

Introduction

Mancroft Advice Project (MAP) delivers a range of services supporting children, young people, and vulnerable adults, including youth work, therapeutic support, advice services, alternative provision, community-based delivery, outreach, and online engagement.

Digital technology and online communication form an important part of how MAP delivers support, maintains relationships, stores information, and engages with service users, families, professionals, and partner organisations.

MAP recognises that online environments present both opportunities and risks. Online safety is therefore viewed as a safeguarding responsibility across the whole organisation and not solely as an IT or technical issue.

This policy outlines how MAP seeks to:

- Protect children, young people, vulnerable adults, staff, and volunteers when using digital technology and online platforms.
- Promote safe, professional, and respectful online behaviour.
- Reduce risks associated with online harm, cyber incidents, inappropriate communication, exploitation, bullying, radicalisation, and breaches of confidentiality.
- Ensure staff understand their responsibilities in relation to online safeguarding, cyber security, professional boundaries, and data protection.
- Support a culture of vigilance, accountability, and safe digital practice across all services.

This policy applies to Employees, Volunteers, Contractors and agency staff, Trustees where relevant to their role.

Four key areas of online risk

MAP recognises four key categories of online risk:

- **Content** - Exposure to harmful, inappropriate, misleading, or illegal material.
- **Contact** - Being subjected to harmful interaction online including bullying, exploitation, coercion, or grooming.
- **Conduct** - Unsafe or inappropriate online behaviour by individuals.
- **Commerce** - Risks linked to scams, gambling, financial exploitation, advertising, or misuse of personal data.
- Where possible staff will provide education, guidance, supervision, and intervention proportionate to the needs and vulnerabilities of service users.

Roles and Responsibilities

Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for safeguarding and online safety within MAP.

DSL:

Darren Cox – Director of Operations / Designated Safeguarding Lead

Dan Mobbs – CEO / Designated safeguarding lead.

Online Safety and Safeguarding Principles

MAP recognises that online risks can significantly impact wellbeing, safety, mental health, relationships, and service engagement.

Online safeguarding includes protecting individuals from:

- Bullying, harassment, or intimidation
- Grooming, exploitation, or coercion
- Exposure to harmful or inappropriate content
- Radicalisation and extremist material
- Online abuse or manipulation
- Fraud, scams, phishing, or cybercrime
- Breaches of confidentiality or misuse of personal information
- Unsafe or inappropriate communication

MAP also recognises that online harms are often linked to wider contextual safeguarding concerns including peer relationships, exploitation, family circumstances, mental health, social isolation, and community risks.

Professional Boundaries and Communication

Staff, volunteers, and representatives of MAP must maintain clear professional boundaries at all times when communicating online.

Staff must:

- Use approved MAP systems and communication methods only.
- Use work email accounts and approved platforms for service-related communication.
- Devices
- Maintain professional language, behaviour, and conduct online.
- Report concerns, inappropriate communication, or boundary issues immediately.

Staff must not:

- Use personal social media accounts to communicate with service users.
- Share personal phone numbers unless formally authorised.
- Engage with children or young people through gaming platforms or unofficial messaging applications.
- Store sensitive information on personal devices or unapproved systems.
- Share screenshots, recordings, or information relating to service users without authorisation.

Where platforms such as Microsoft Teams, WhatsApp Business, spond, text messaging, or online learning systems are used, this must be in line with MAP procedures and risk-assessed service delivery.

Safe Online Delivery

MAP delivers some services through digital and online platforms including:

- Online meetings
- Remote support sessions
- Therapeutic interventions
- Group work
- Youth engagement activities
- Alternative provision and learning activities

To support safe online delivery:

- Only approved and secure platforms will be used.
- Access links and invitations must be shared appropriately.
- Staff must consider privacy, confidentiality, and safeguarding when facilitating online sessions.
- Online sessions must remain professional, purposeful, and appropriate to the needs of service users.
- Concerns arising during online delivery must be responded to in line with safeguarding procedures.

MAP does not routinely record online sessions. Any recording must:

- Have a clear and justifiable purpose,
- Comply with data protection requirements,
- Be communicated clearly to participants where appropriate.

Cyber Security and Data Protection

MAP recognises that cyber security incidents can present safeguarding, operational, and reputational risks. MAP will take reasonable and proportionate steps to protect systems, devices, accounts, and sensitive information.

This includes:

- Password protection and multi-factor authentication where appropriate.
- Staff cyber security awareness training including penetration testing
- Monitoring and responding to phishing attempts and suspicious activity.
- Secure storage and management of information through approved systems.
- Appropriate access controls and permissions.
- Reporting and investigating suspected breaches or cyber incidents promptly.

All staff are responsible for:

- Remaining vigilant to phishing emails and scams.
- Protecting login credentials and devices.
- Following MAP data handling and IT procedures.
- Reporting any suspected breach, loss of data, or unauthorised access immediately.

Failure to follow cyber security expectations may be treated as a disciplinary matter where appropriate.

Working with Families and Professionals

MAP recognises the importance of collaborative safeguarding. Where appropriate, MAP will work with Parents and carers, Schools and education providers, Social care, Health professionals, Youth justice services, Police and other partner agencies. This may include sharing concerns relating to online safety where lawful, necessary, and proportionate to protect welfare and safety.

Training and Awareness

MAP will ensure:

- Staff receive safeguarding and online safety training appropriate to their role.
- Online safety is embedded within induction processes.
- Staff understand reporting procedures and professional expectations.
- Learners and service users receive appropriate online safety education and support where relevant.

Reporting Concerns

Any concerns relating to online safety, inappropriate online behaviour, cyber incidents, or digital safeguarding must be reported immediately in line with MAP safeguarding procedures.

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Data Protection and Confidentiality Policy
- Staff Code of Conduct
- Acceptable Use of Technology Policy
- Behaviour and Anti-Bullying Policy
- Whistleblowing Policy

Legislative and Statutory Framework

This policy is informed by:

- Keeping Children Safe in Education (KCSIE, 2026)
- Working Together to Safeguard Children (2023)
- UK GDPR and Data Protection Act 2018
- Prevent Duty Guidance
- Counter-Terrorism and Security Act 2015
- Children Acts 1989 and 2004
- Norfolk Safeguarding Children Partnership guidance
- Cyber security guidance issued by the National Cyber Security Centre (NCSC)

This master document is controlled electronically. Printed copies or copies saved by individuals are not controlled. Document users are responsible for ensuring copies are valid prior to use. This policy will be monitored through: SMT / practitioner oversight.

Author – name and title	Darren Cox, Director of Operations
Date issued	30 th November 2025
Next review date	31 st October 2026