e–Safety Policy

Contents

Summary Table

Policy Title	e-Safety Policy v7		
Policy Number	015a v7	**Date of Approval**	23 Aug 2024
Effective Date	23 Aug 2024	**Date for Review**	23 Aug 2025
Approver	Derek Meier	**Policy Owner**	Derek Meier

Document History

Date	Document Version	Document Revision Description	Document Author	Approved By
02 Dec 2019	1.0	Initial Publication	P Melvin	Ray Johnson
16 Apr 2020	2.0	Updated to reflect business organisation name change	P Melvin	Stuart Milne
01 Apr 2021	3.0	Update of DSO and safeguarding email address	P Melvin	Stuart Milne
16 Sep 2021	4.0	Section 10 Updated to show dedicated safeguarding email address	P Melvin	Derek Meier
15 Jul 2022	5.0	Review and rebranding	S Richards	Derek Meier
04 Aug 2023	6.0	Annual review and update	S Richards	Derek Meier
23 Aug 2024	7.0	Annual review and update	M Guzy	Derek Meier

1. Introduction

Maximus is committed to ensuring that the safety and wellbeing of at risk adults, children, and young people at all times. This includes the process of limiting the risks when using the internet, digital and mobile technologies through implementation of this policy.

We recognise that the online world provides everyone with opportunities; however, it can also present risks and challenges. Maximus has a responsibility to keep at risk adults, children, and young people safe online.

This policy should be read in conjunction with other relevant organisation policies and procedures such the Equality, Diversity and Inclusion Policy, Health and Safety Wellbeing Policy, Dignity at Work Policy, Whistleblowing Policy and Data protection policies and procedures.

2. Purpose

The purpose of this policy is to:

- Ensure the safety and wellbeing of adults at risk, children and young people when using technology, including the internet, social media, or mobile devices.
- Provide the overarching principles that guides our approach to online safety.
- Ensure that a clear and effective robust incident reporting procedure is in place which is communicated across the business and to individuals who access our services.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

3. Definition of e-Safety Risks

The types of e-safety risks can be summarised under the following two headings:

a) Content

- Exposure to socially unacceptable online discriminatory materials which incite violence, hate, extremism, or intolerance.
- Exposure to inappropriate content.
- Exposure to inaccurate or misleading information.
- Illegal downloading of copyrighted materials, e.g., music and films.

b) Contact

- Cyberbullying via websites, mobile phones, or other forms of communications devices.
- Grooming using communications technologies.
- Radicalisation in which a person is coerced into supporting terrorism and extremist ideologies associated with terrorist groups.

4. Scope

This Policy applies to all persons who have authorised access to Maximus services in England, Wales, and Scotland.

This includes those providing services on behalf of the organisation such as service delivery partners, casual workers and agency staff, consultants, contractors, and volunteers. This also includes parents/carers or visitors if they have access to and are users of the organisation IT systems.

5. Roles & Responsibilities

Role	Responsibilities
Designated Safeguarding Lead (DSL)	• Have clear and robust safeguarding procedures in place for responding to safeguarding issues in relation to online abuse. • Making sure our responses take the needs of the person experiencing abuse, any bystanders, and our organisation as a whole into account. • Design and implementation of high-quality safeguarding training to safeguarding advocates which includes e–Safety guidelines. • To liaise with business managers to ensure that colleagues have completed the recommended safeguarding training and are fully informed of online safety requirements. • Working with safeguarding advocates across the business to raise awareness of safeguarding issues arising from the sharing of personal data, access to illegal or inappropriate material, potential grooming, and cyber bullying. • Ensure processes are aligned to current legislation, statutory and other guidance with regards to safeguarding adults at risk, children, and young people. • To ensure that there is a mechanism to report online safety issues with partner organisations and those who provide services on our behalf. • To take the lead role in managing the day-to-day online safety issues. • Liaise with Safeguarding Advocates and Information Security Manager in relation to online e-Safety issues.
Designated Safeguarding Officer (DSO)	• Support the Designated Safeguarding Lead in the above duties.

Safeguarding Advocates	• Support individual colleagues in the completion of the safeguarding report forms, where applicable, and email all reports to safeguarding@maximusuk.co.uk. The safeguarding report will be ongoing until both Advocate and Designated Safeguarding Officer agree case closure.
Maximus Colleagues	• Read and understand the e-Safety Policy, Safeguarding Policies and Procedures Equality, Diversity and Inclusion Policy, Health and Safety Wellbeing Policy, Dignity at Work Policy, Whistleblowing Policy and Data protection policies and procedures. • Promote and follow the organisation's mission and values at all times, including professionalism in the use of their own technology. • Ensure that no references are made to participants on social media and do not engage in online discussions in relation to personal matters in relation to participants. • Support and encourage adults, children and young people accessing our services to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others. • Provide support and guidance to participants in identifying the forms of abuse, including bullying, cyberbullying, grooming and radicalisation. • Ensure participants are aware that there will be a zero tolerance in relation to online abuse. • Report any suspected misuse or issues to their line manager and the Designated Safeguarding Lead and/or Designated Safeguarding Officer/s who will provide advice and guidance and lead on reporting any online abuse. • Understand that any unacceptable online behaviour and actions conducted by colleagues could lead to disciplinary procedures.

Participants	• Ensure that the guidance is understood and followed in relation to e-Safety and understand how to use technology that keeps them safe and shows respect for others. • Read and understand the online safety guidance held within Welcome Packs, online safety poster guidance and advice and guidance held on computer stations. • Follow the online safety processes when accessing digital technologies provided. • Understand the risks associated with the downloading, posting, and sharing and posting of images, including their own, on social networking sites. • Knowledge that the use of images or photographs is encouraged in learning and support, providing there is no breach of copyright. • Understanding that we will request permission and obtain signed consent from the participant (or parents if the participant is under 18 years) before photographs or information e.g., good news stories are published on the organisation's website.

6. Aims

- To ensure that safeguarding within the organisation's IT systems is strong and dependable.
- To ensure that the storage and use of images and personal information on the organisation's IT systems is secure and meets all legal requirements.
- Assurance that there is one single point of contact (Designated Safeguarding Team) who will manage any issues involving online abuse and will report to IT and the relevant members of senior leadership.
- That there is a robust system in place to minimise the risk of online abuse.
- To educate online safety across the business and to individuals who access our services.

- To ensure that any online incidents which threaten e-safety are managed appropriately.

7. Outcomes

a) Security

- Maximus services are safe and secure with appropriate and up to date security measures and software in place.

b) Behaviours

- All users of technology adhere to the standards of behaviour set out in the User Information Security Policy and how to comply with the Information Security Incident and Reporting Process.

- It is unacceptable for all users of technology to download or transmit any material which might be considered obscene, abusive, sexist, racist, defamatory, related to extremism or terrorism or which is intended to annoy, harass, or intimidate another person; this also applies to the use of social media systems accessed from the organisation's systems.

- The use of technology adheres to the organisation's guidelines when using email, mobile phones, social networking sites, chat rooms, video conferencing and web cameras etc.

- Any abuse of IT systems and any issues relating to online abuse are dealt with seriously in line with the organisation's disciplinary procedures.

- Any conduct that is considered illegal is reported to the police.

8. Process

Any concerns identified relating to e-safety should be reporting following the Safeguarding Policies and Procedures.