RESET

SEMH

Reset-Recharge-Refocus

E-Safety Policy

Date: 30/03/2025
Renewed Date: 30/03/2026
Reviewed by Karen Birch 30/03/2025

Reset AP Ltd

1. Introduction

Reset AP Ltd is committed to ensuring the safety and well-being of all employees, clients, and stakeholders when using digital technologies. This policy outlines the principles and guidelines for maintaining a safe and secure online environment.

2. Scope

This policy applies to all employees, contractors, and clients using Reset AP Ltd.'s IT systems, digital platforms, and online services. It covers the use of:

- Company-provided devices and networks
- Personal devices used for company-related work
- Email, social media, and online communications
- Cloud-based services and data storage

3. Key Principles

- Protecting Data & Privacy: All personal and business-sensitive information must be handled securely.
- Responsible Use: Employees must use IT resources responsibly and ethically.
- Cybersecurity Measures: Staff must follow best practices to prevent cyber threats.
- Safeguarding: Measures are in place to protect employees, clients, and partners from online harm.

4. Acceptable Use Guidelines

- Use company devices and networks for business-related activities only.
- Do not share login credentials or sensitive company information.
- Be cautious when opening emails or links from unknown sources.
- Ensure that all software and security updates are installed promptly.
- Use strong passwords and enable multi-factor authentication where possible.

5. Social Media and Online Conduct

- Employees must represent Reset AP Ltd professionally on social media.
- Personal opinions should not be misrepresented as company views.
- No engagement in cyberbullying, harassment, or sharing of inappropriate content.
- Confidential company information should never be disclosed online.

6. Cybersecurity & Data Protection

- All devices must have up-to-date antivirus and security software.
- Employees must report any suspicious activity, phishing attempts, or data breaches immediately.
- Use encrypted communication channels when sharing sensitive data.
- Regular security awareness training will be conducted.

7. Safeguarding and Online Safety

- Employees must be aware of the risks of online grooming, fraud, and exploitation.
- Any concerns related to online safety should be reported to the designated e-safety officer.
- Content filtering and monitoring may be used to prevent access to harmful or inappropriate material.

8. Incident Reporting & Response

- Any breaches of this policy must be reported to the IT/security team immediately.
- Investigations will be conducted to assess and mitigate risks.
- Disciplinary action may be taken for violations of this policy.

9. Review & Compliance

- This policy will be reviewed annually to stay up to date with technological and legal changes.
- Compliance with this policy is mandatory, and failure to adhere may result in disciplinary action.

RESET
SEMH
Reset-Recharge-Refocus