

Remedicare Education Services

Online Safety and Acceptable Use Policy

Publication Date: September 2026

Review Date: September 2027

1. Introduction

Remedicare Education Services is committed to ensuring that all learners and staff can benefit from the opportunities provided by digital technology while remaining safe and protected from online harm.

As an Alternative Provision provider, Remedicare recognises that many learners may require additional support to understand online risks, develop safe digital behaviours and navigate online relationships.

Technology is an important part of education, communication and daily life. However, online environments can present safeguarding risks including:

- Cyberbullying.
- Online grooming.
- Exploitation.
- Harmful content.
- Online harassment.
- Sharing of inappropriate images.
- Misinformation.
- Privacy risks.
- Excessive or unsafe use of technology.
- Risks associated with Artificial Intelligence (AI).

This policy outlines how Remedicare Education Services promotes safe, responsible and respectful use of technology.

This policy should be read alongside:

- Child Protection & Safeguarding Policy.
- Staff Code of Conduct.
- Anti-Bullying Policy.
- Behaviour Support Policy.
- GDPR/Data Protection Policy.
- Whistleblowing Policy.

2. Scope

This policy applies to:

- All learners attending Remedicare Education Services.
- All staff.
- Volunteers.
- Contractors.
- Visitors where technology is used.
- All Remedicare devices and systems.
- Personal devices used for educational purposes.
- Online platforms and communication systems.

3. Our Online Safety Principles

Remedicare Education Services expects everyone to:

- Use technology safely and responsibly.
- Respect others online and offline.
- Protect personal information.
- Report concerns immediately.
- Follow staff guidance.
- Understand that online behaviour can have safeguarding consequences.

4. Roles and Responsibilities

Directors and Senior Leadership Team

Responsible for:

- Ensuring online safety remains a safeguarding priority.
- Ensuring appropriate systems and procedures are in place.
- Ensuring staff receive appropriate training.
- Reviewing online safety incidents.

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Managing online safeguarding concerns.

- Supporting staff with online safety issues.
- Making referrals where required.
- Ensuring incidents are recorded.
- Working with external agencies.

Staff Responsibilities

Staff must:

- Model safe and responsible digital behaviour.
- Supervise learners appropriately when using technology.
- Report online safety concerns immediately.
- Follow acceptable use expectations.
- Maintain professional boundaries online.

Staff must not:

- Communicate with learners through personal social media accounts.
- Share personal information with learners.
- Use inappropriate websites or content around learners.
- Photograph learners using personal devices.

5. Learner Responsibilities

Learners are expected to:

- Use technology respectfully.
- Follow staff instructions.
- Report anything that makes them feel unsafe.
- Respect other people's privacy.
- Use devices appropriately.

6. Mobile Phone and Personal Device Procedure

Purpose

At Remedicare Education Services, we recognise that mobile phones and personal smart devices are an important part of everyday life. However, these devices can also create safeguarding risks, impact emotional regulation, affect learning and create challenges around privacy, relationships and online safety.

As an Alternative Provision supporting learners with a range of individual needs, Remedicare takes a personalised and risk-based approach to mobile phone use.

This procedure aims to:

- Protect learners and staff from online safety risks.
- Support positive learning environments.
- Reduce distractions and emotional barriers to learning.
- Promote safe and responsible use of technology.
- Support learners to develop appropriate digital behaviours.

This procedure should be read alongside the Remedicare Online Safety and Acceptable Use Policy, Child Protection & Safeguarding Policy and Staff Code of Conduct.

Primary Learners

Remedicare Education Services operates a **mobile-phone-free environment for all Primary learners** attending the provision.

Primary learners must not bring personal mobile phones or smart devices into the provision.

This includes:

- Mobile phones.
- Smart watches with messaging, internet access, cameras or recording functions.
- Personal tablets.
- Personal internet-enabled devices.

This approach supports:

- Safeguarding.
- Emotional wellbeing.
- Positive relationships.
- Engagement in learning.
- Reduced exposure to online risks.

Parent and Carer Responsibilities – Primary Learners

Parents and carers play an important role in supporting this safeguarding procedure.

Parents/carers must ensure that:

- Primary learners do not bring mobile phones or smart devices into the provision.
- Mobile phones remain with parents/carers during drop-off and collection.
- Devices are not given to learners while they are attending Remedicare.

Remedicare Education Services cannot accept responsibility for loss, damage or theft of personal devices brought onto the provision site.

If a Primary Learner Brings a Mobile Phone or Smart Device

If a Primary learner arrives with a mobile phone or smart device:

- A member of staff will safely secure the device.
- The device will be stored securely during the learner's attendance.
- Parents/carers will be informed.
- The device will be returned through agreed arrangements.

Repeated incidents will be discussed with parents/carers to ensure expectations are understood.

Where there are exceptional circumstances, arrangements may be agreed with the DSL and senior leadership team.

Secondary Learners

Remedicare recognises that some Secondary learners may have a legitimate reason for carrying a mobile phone, including:

- Independent travel arrangements.
- Communication with parents/carers.
- Medical needs.
- Safeguarding considerations.
- Preparation for adulthood and independence.

However, mobile phone use must remain appropriate and must not impact:

- Learning.
- Safety.
- Relationships.
- Emotional wellbeing.
- The privacy of others.

Expectations for Secondary Learners

Secondary learners may bring mobile phones to Remedicare; however:

Learners must:

- Follow staff instructions regarding phone use.
- Keep devices stored appropriately when requested.
- Use phones respectfully and safely.
- Protect personal information.
- Report online safety concerns.

Learners must not:

- Use phones during learning sessions unless agreed by staff.
- Photograph or record learners or staff.
- Share images or recordings without consent.
- Access inappropriate content.
- Use devices to bully, threaten or harm others.
- Communicate with staff through personal accounts or messaging platforms.

Managing Inappropriate Mobile Phone Use – Secondary Learners

Where mobile phone use becomes a concern, Remedicare may introduce additional support measures.

These may include:

- A verbal reminder of expectations.
- Increased monitoring.
- The phone being stored securely during sessions.
- An individualised mobile phone agreement.
- Discussion with parents/carers.
- Inclusion within a learner support or behaviour plan.

Any response will consider the learner's individual needs, communication profile and circumstances.

Safeguarding Concerns Involving Mobile Phones

Mobile phones and smart devices can present safeguarding risks, including:

- Cyberbullying.

- Online harassment.
- Sharing inappropriate images.
- Access to harmful content.
- Grooming or exploitation.
- Recording others without consent.
- Online conflict between learners.

Where staff identify a safeguarding concern linked to mobile phone use, this must be reported immediately to the DSL/DDSL team and managed in line with the Child Protection & Safeguarding Policy.

Staff Responsibilities

All Remedicare staff must:

- Apply mobile phone expectations consistently.
- Model appropriate technology use.
- Maintain professional boundaries.
- Report safeguarding concerns.
- Ensure learner privacy is protected.

Staff must not:

- Use personal devices to photograph learners.
- Store learner information on personal devices.
- Communicate with learners through personal social media or messaging accounts.
- Share learner images or information without appropriate authorisation.

Exceptional Circumstances

In exceptional circumstances, a learner may require access to a mobile phone or smart device due to:

- Medical needs.
- Specific safeguarding arrangements.
- Communication needs.
- Travel requirements.

Any agreed exception must:

- Be approved by senior leadership and/or the DSL.
- Be recorded.
- Include clear expectations for use.

- Be reviewed regularly.

Key Message

Remedicare Education Services recognises the importance of technology while ensuring learner safety remains the priority.

Mobile phones and personal devices must always be managed in a way that promotes:

- Safeguarding.
- Respect.
- Learning.
- Emotional wellbeing.
- Positive relationships.

7. Photography, Recording and Images

Learners and staff must not:

- Take photographs of others without permission.
- Record staff or learners.
- Share images online without consent.

Staff must only use approved devices and systems.

Any concerns involving images or recordings must be reported immediately.

8. Social Media

Learners should understand that online behaviour can impact:

- Their safety.
- Their relationships.
- Their education.
- Other people's wellbeing.

Learners must not:

- Share harmful content.
- Bully others online.
- Share private information.

- Create accounts to target others.

Staff must:

- Maintain professional boundaries.
- Not accept learner requests on personal accounts.
- Not communicate with learners through personal messaging platforms.

9. Artificial Intelligence (AI)

Remedicare recognises that Artificial Intelligence is increasingly used in education and everyday life.

AI can provide positive opportunities, including:

- Supporting learning.
- Improving accessibility.
- Supporting communication.
- Creating educational resources.

However, AI also creates safeguarding risks including:

- Creating false information.
- Sharing personal information.
- Generating inappropriate content.
- Creating fake images or videos.
- Misuse for bullying or harassment.
- Over-reliance on AI instead of developing skills.

Learner Use of AI

Learners must:

- Use AI responsibly.
- Follow staff instructions.
- Not enter personal information into AI tools.
- Not use AI to create harmful content.
- Be honest where AI has supported their work.

Staff Use of AI

Staff may use AI tools to support professional practice where appropriate.

Staff must:

- Not enter confidential learner information into public AI systems.
- Check accuracy of AI-generated information.
- Ensure resources are suitable for learners.
- Follow GDPR requirements.
- Maintain professional judgement.

AI must not replace professional decision-making.

10. Filtering and Monitoring

Remedicare Education Services uses appropriate filtering and monitoring systems to reduce exposure to harmful online content.

Staff should remain aware that filtering systems cannot remove all risks.

Any concerning online activity must be reported to the DSL.

11. Online Bullying and Harmful Behaviour

Online bullying includes:

- Hurtful messages.
- Sharing images without consent.
- Online threats.
- Excluding others.
- Spreading rumours.

Online bullying will be managed in line with:

- Anti-Bullying Policy.
- Child Protection & Safeguarding Policy.

12. Online Safety Education

Remedicare will support learners through:

- Personal development sessions.
- Relationship education.
- Digital citizenship activities.

- Individualised support.
- Communication approaches appropriate to learner need.

Topics include:

- Online relationships.
- Privacy.
- Cyberbullying.
- Digital footprints.
- AI awareness.
- Online exploitation.

13. Reporting Online Safety Concerns

Concerns should be reported to:

- A trusted member of staff.
- DSL/DDSL team.

Staff must record safeguarding concerns appropriately.

Examples include:

- Online grooming.
- Sexual content.
- Threats.
- Exploitation.
- Harmful communication.

14. Confidentiality and Data Protection

Everyone must protect personal information.

Staff and learners must not:

- Share passwords.
- Share confidential information online.
- Upload learner information to unauthorised platforms.

All information must be handled in line with GDPR requirements.

15. Review

This policy will be reviewed annually or sooner if required due to:

- Changes in technology.
- Changes in legislation.
- New safeguarding risks.
- Learning from incidents.