



Reconnect Learning Social Media Policy

Version 1.0 | Effective: September 2026 | Review: September 2027 | Policy Owner: Ellen Kerr, Managing Director & DSL

1. Policy Statement

Our Commitment

Reconnect Learning recognises that social media can be a valuable tool for communication, education, engagement, marketing and professional networking.

This policy ensures that social media is used safely, responsibly and professionally by all staff, tutors, volunteers and contractors associated with Reconnect Learning.

What This Policy Covers

The organisation is committed to protecting learners, staff, families and the reputation of Reconnect Learning whilst promoting the safe and effective use of digital platforms.

This policy applies to both **professional and personal use** of social media where such use may impact Reconnect Learning, its learners, staff or stakeholders.

2. Purpose

This policy aims to achieve the following key objectives across all areas of social media use within Reconnect Learning.



Promote Safe Use

Promote safe and responsible social media use across the organisation.



Protect Children

Protect children and young people from online harm and exploitation.



Safeguard All

Safeguard staff and learners in all digital environments.



Professional Boundaries

Maintain professional boundaries between staff and learners at all times.



Protect Information

Protect confidential information and comply with data protection requirements.



Protect Reputation

Protect the reputation of Reconnect Learning and ensure compliance with safeguarding requirements.

3. Scope

Who This Policy Applies To

- Employees
- Tutors
- Volunteers
- Contractors & Agency Staff
- Directors

What It Covers

Professional
social media use

Personal social
media use where
it impacts
Reconnect
Learning

Social
networking sites
& messaging
applications

Video sharing
platforms &
online forums

Blogging
platforms &
discussion
groups

4. Legal and Regulatory Framework

This policy has regard to the following legislation and statutory guidance:

Statutory Guidance

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Prevent Duty Guidance (current version)
- Children Act 1989
- Children Act 2004

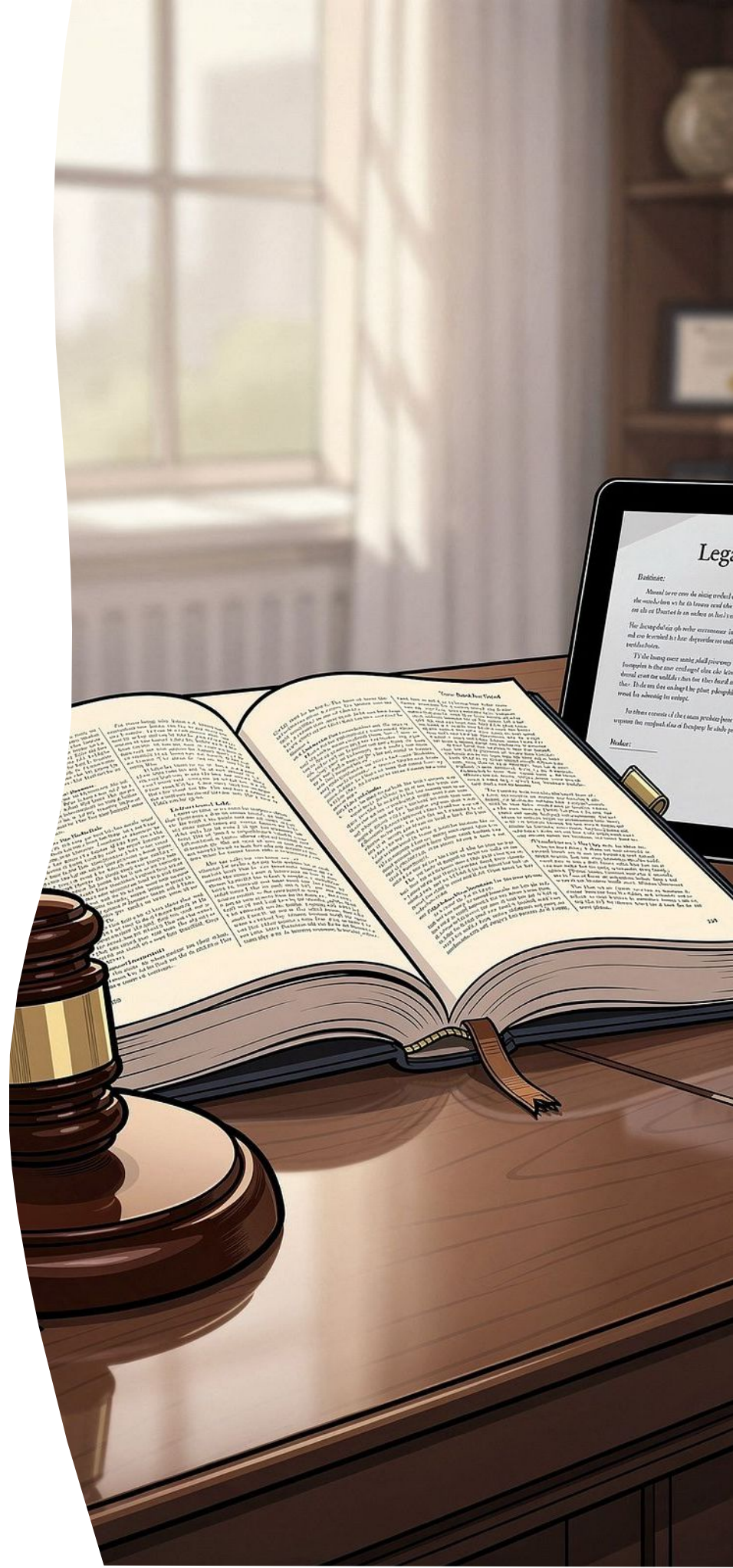
Data & Privacy

- Data Protection Act 2018
- UK GDPR
- Human Rights Act 1998

Equality & Online Safety

- Equality Act 2010
- Online Safety Act 2023
- Prevent Duty Guidance

This policy should be read alongside Reconnect Learning's Safeguarding and Child Protection Policy, which is the organisation's overarching safeguarding policy.



5. Definitions — What Is Social Media?

Social media includes, but is not limited to, the following platforms. New and emerging platforms are also covered by this policy.



Social Networks

Facebook, Instagram, X (formerly Twitter), LinkedIn, TikTok, Snapchat



Messaging Apps

WhatsApp, Telegram, Discord, and other private or group messaging platforms



Video Platforms

YouTube and other video sharing or live streaming services



Blogs & Forums

Blogging platforms, online forums, professional networking sites and discussion groups



This policy covers all current and future platforms. If in doubt about whether a platform is covered, assume that it is and seek guidance from the Director.

6. Professional Conduct

Online conduct should reflect the same professional standards expected in face-to-face interactions. Staff must always consider how their content may be perceived by others.

1 Act Professionally at All Times

Maintain public confidence and behave in a manner consistent with Reconnect Learning values in all online spaces.

2 Consider How Content May Be Perceived

Before posting, consider whether the content could be misinterpreted or cause harm to learners, colleagues or the organisation.

3 Protect the Welfare of Learners

Learner welfare must always take priority. Maintain appropriate professional boundaries in all online interactions.

7. Professional Boundaries

- ⊗ Staff must never use personal social media accounts to communicate with learners. All communication must occur through approved organisational systems and channels only.

Staff Must NOT:

Accept personal
friend requests
from learners

Send personal
friend requests to
learners

Engage in private
social media
conversations
with learners

Share personal
contact details
with learners

Communicate
with learners
through personal
social media
accounts

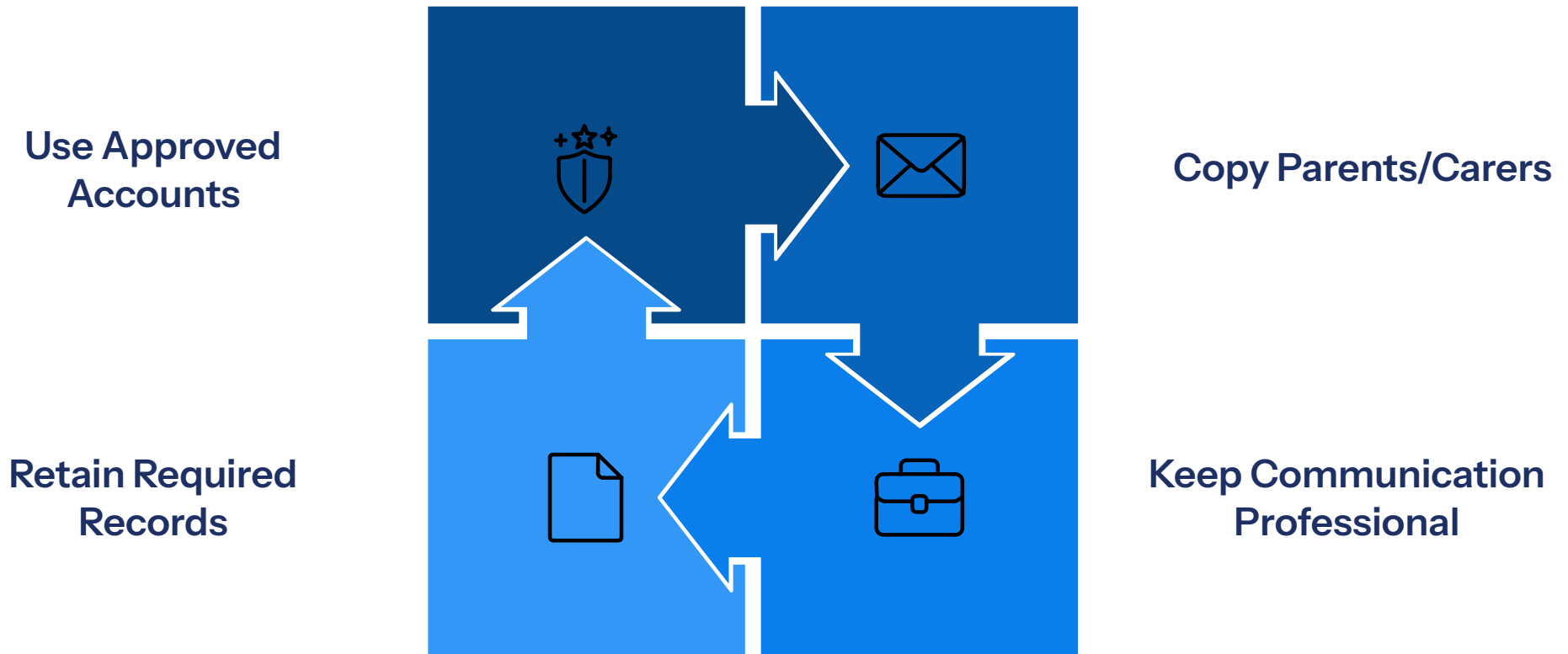
The Golden Rule

Professional boundaries must always be maintained. When in doubt, do not engage — seek guidance from the Managing Director before proceeding.

Communication with learners must only occur through **approved organisational systems and communication channels**. This protects both learners and staff.

8. Communication with Learners

Reconnect Learning recognises that online communication may form part of educational provision. Where communication is required, the following standards apply.



This process ensures all learner communications are transparent, appropriate and auditable. Staff must **never use disappearing message functions** when communicating about learners.



9. Personal Use of Social Media

Reconnect Learning respects employees' rights to personal social media use. However, staff should be mindful of the following responsibilities. Personal accounts remain the responsibility of the account holder.

1

Review Privacy Settings

Regularly review and update privacy settings on all personal accounts to limit public visibility.

2

Avoid Identifying Learners

Never identify, tag or reference learners in personal social media posts or content.

3

Avoid Work-Related Discussions

Do not discuss work-related matters or share confidential information on personal accounts.

4

Consider Professional Reputation

Consider how personal posts may reflect on your professional reputation and on Reconnect Learning.

10. Protecting Learners

- ❌ Learner welfare must always take priority. Any breach of learner privacy online may constitute a safeguarding concern and will be treated accordingly.

Staff must never engage in any of the following activities relating to learners on social media:

No Photographs Without Consent

Never share learner photographs without appropriate, documented consent from parents or carers.

No Personal Information

Never share learner personal information, circumstances or identifying details online.

No Safeguarding Discussions

Never share safeguarding concerns or sensitive information through social media channels.

No Identifying Content

Never publish any content that could identify a learner without explicit authorisation.

11. Safeguarding and Social Media

Social media can present significant safeguarding risks. Staff must be vigilant and report any concerns identified through social media in accordance with safeguarding procedures.



⚠ Any safeguarding concern identified through social media must be reported immediately to the Managing Director & Designated Safeguarding Lead (DSL) and managed in accordance with the Safeguarding and Child Protection Policy.

12. Cyberbullying

Reconnect Learning will not tolerate cyberbullying in any form involving learners, staff, families or partner organisations.

Zero Tolerance

Reconnect Learning takes a firm zero-tolerance approach to cyberbullying. All concerns must be reported immediately to the Managing Director.

Cyberbullying may be treated as a safeguarding concern and may result in formal action.

Cyberbullying May Include:

- Threatening messages or communications
- Harassment and persistent unwanted contact
- Creation of fake accounts to impersonate or harm
- Sharing harmful, humiliating or degrading content
- Deliberate exclusion from online groups
- Any content designed to intimidate or distress

13. Photography, Video and Media Content

Photographs, videos and media content may only be used where all of the following conditions are met:



Appropriate Consent Obtained

Written consent must be obtained from parents or carers before any images of learners are captured or shared.



Content Is Suitable and Professional

All media content must be appropriate, professional and reflect the values of Reconnect Learning.



Learner Dignity Maintained

Content must always maintain the dignity and respect of learners at all times.



Safeguarding Risks Considered

A safeguarding risk assessment must be considered before any media content is captured or published.

⊗ Images must never compromise the safety or privacy of learners under any circumstances.



14. Organisational Social Media Accounts

Official Reconnect Learning social media accounts may be used for the following purposes. Only authorised individuals may manage organisational accounts.

Marketing

Promoting Reconnect Learning services and programmes to prospective learners and families.

Information Sharing

Sharing relevant updates, news and information with learners, families and stakeholders.

Educational Content

Publishing educational resources and content that supports learner development.

Community Engagement

Building relationships with the wider community and partner organisations.

Recruitment

Advertising vacancies and promoting Reconnect Learning as an employer of choice.

Celebrating Achievements

Recognising and celebrating the achievements of learners and staff (with appropriate consent).

15. Content Standards

Content shared through organisational accounts must meet the following standards and support the positive reputation of Reconnect Learning.

	Accurate All content must be factually correct and verified before publication.
	Respectful Content must treat all individuals with dignity and respect.
	Inclusive Content must reflect the diversity of our learners and communities.
	Values-Aligned Content must reflect the organisational values of Reconnect Learning.
	Safeguarding-Aware Content must promote safeguarding and wellbeing at all times.
	Non-Discriminatory Content must never include discriminatory, offensive or harmful material.

Artificial Intelligence (AI) and Generated Content

Staff must ensure that any AI-generated content shared through organisational social media accounts is accurate, appropriate, professionally reviewed and compliant with safeguarding, confidentiality and data protection requirements. AI-generated images or content must not misrepresent learners, staff or organisational activities. AI-generated images must never be used to represent actual learners unless clearly identified as illustrative content and appropriate permissions have been obtained where applicable.

16. Confidentiality and Data Protection

- ⊗ All social media activity must comply with the Data Protection Act 2018, UK GDPR and all confidentiality obligations. Breaches may result in formal action and referral to the Information Commissioner's Office (ICO).

Staff Must Never Share:

- Confidential information of any kind
- Personal data relating to learners or staff
- Safeguarding records or case information
- Internal documents without authorisation

Compliance Requirements

All social media activity must comply with:

- **Data Protection Act 2018** — governing how personal data is handled
- **UK GDPR** — setting out rights and responsibilities for data processing
- **Confidentiality obligations** — as set out in contracts of employment and organisational policies

Records relating to safeguarding concerns, social media incidents, cyberbullying reports, investigations, approvals, organisational communications and associated documentation will be retained in accordance with Reconnect Learning's Records Retention Schedule, the Data Protection Act 2018 and UK GDPR.

17. Use of Messaging Applications

Messaging applications such as WhatsApp, Microsoft Teams, Zoom Chat and Google Chat must only be used in accordance with organisational procedures. All approved messaging platforms must comply with Reconnect Learning's data protection, safeguarding and record-retention requirements.

Use Professional Accounts

Use professional accounts where possible and avoid mixing personal and professional communications.

Maintain Professional Language

All communications must use professional language appropriate to an educational setting.

Avoid Personal Discussions

Messaging applications must not be used for personal discussions or non-work-related content.

Ensure Appropriateness

All communications must remain appropriate and consistent with organisational values.

- ❏ Group communications should be transparent and auditable. Staff must never use disappearing message functions when communicating about learners or organisational matters.

18. Reputational Risk

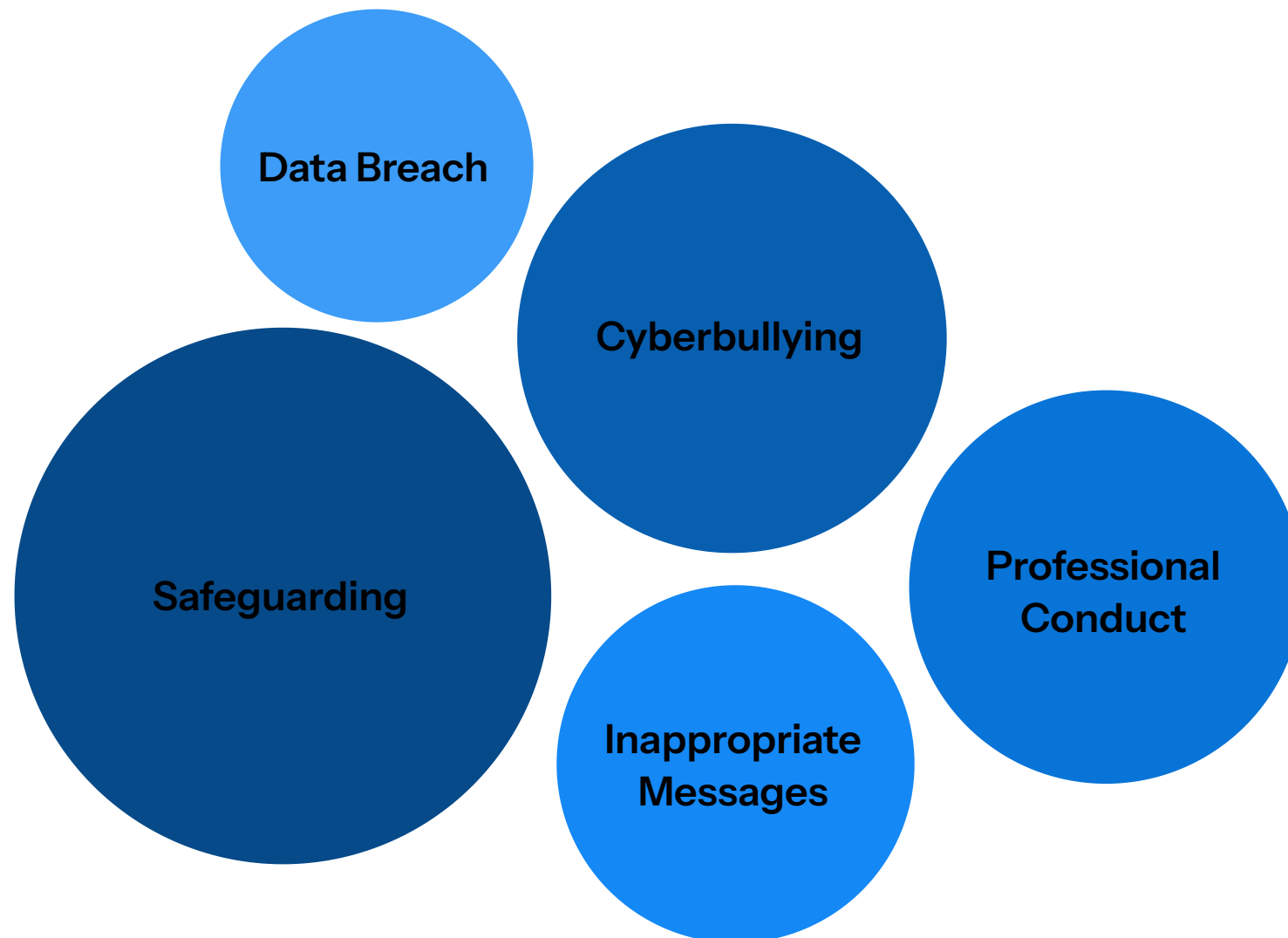
Staff remain personally responsible for all content they publish online. The following types of content must be avoided at all times.



 Staff remain personally responsible for content they publish, even on personal accounts, where that content may impact Reconnect Learning or its learners.

19. Reporting Concerns

All concerns relating to social media must be reported immediately to the Managing Director & Designated Safeguarding Lead (DSL). Do not delay reporting — early intervention is critical.



Report To:

Ellen Kerr — Managing Director & DSL
Reconnect Learning
Email: info@reconnectlearning.co.uk

Important Reminder

Safeguarding concerns must be managed in accordance with the Safeguarding and Child Protection Policy. Do not attempt to investigate safeguarding concerns independently — always refer to the Managing Director & DSL immediately.

20. Monitoring

Reconnect Learning reserves the right to monitor social media activity in accordance with the following principles. All monitoring will be proportionate and lawful.

Monitor Official Accounts

Reconnect Learning will monitor all official organisational social media accounts on an ongoing basis.

Investigate Concerns

Where concerns are raised, the organisation reserves the right to investigate and review relevant communications.

Review Public Information

Publicly available information may be reviewed where concerns arise regarding staff conduct or learner safety.

Take Appropriate Action

Where policies are breached, appropriate action will be taken in accordance with organisational procedures.

21. Breaches of This Policy

- ❌ Serious breaches of this policy may be treated as safeguarding concerns and referred to relevant authorities, including the Local Authority Designated Officer (LADO) where appropriate.

Failure to comply with this policy may result in the following actions, depending on the nature and severity of the breach:



Additional Training



Supervision



Formal Management Action



Referral to Relevant Authorities



Termination of Contract

22. Training and Awareness

All staff will receive guidance and awareness training relating to social media safety and professional conduct. Training records will be maintained by the Managing Director.



23. Monitoring and Review

The Managing Director will monitor all aspects of social media policy compliance and organisational account activity. This policy will be reviewed annually and without unnecessary delay following changes to legislation, statutory guidance, safeguarding practice, online safety risks, organisational arrangements or learning identified through incidents, audits, inspections, complaints, monitoring or service reviews.

The Managing Director Will Monitor:

- Social media concerns and incidents
- Safeguarding incidents linked to social media
- Organisational account activity
- Policy compliance across all staff
- Training completion records

Review Schedule

This policy will be reviewed annually and without unnecessary delay following changes to legislation, statutory guidance, safeguarding practice, online safety risks, organisational arrangements or learning identified through incidents, audits, inspections, complaints, monitoring or service reviews.

Next Review Date: September 2027

24. Related Policies

This policy should be read alongside the following organisational policies. Together, these policies form a comprehensive framework for safe and professional practice at Reconnect Learning.



Safeguarding and Child Protection Policy



Online Safety Policy



Staff Code of Conduct



Data Protection & GDPR Policy



Whistleblowing Policy



Positive Behaviour Support Policy



Anti-Bullying Policy



Complaints Policy



Photography & Media Consent Policy



Mental Health & Wellbeing Policy

Compliance Status

This policy has been developed with regard to the relevant legislation, statutory guidance and governance expectations applicable at the date of approval and will be reviewed following significant legislative or regulatory changes.

KCSIE 2026

Keeping Children Safe in Education
(KCSIE) 2026

Working Together 2026

Working Together to Safeguard
Children 2026

Online Safety Act 2023

Online Safety Act 2023

Data Protection Act 2018

Data Protection Act 2018

UK GDPR

UK General Data Protection
Regulation

Equality Act 2010

Equality Act 2010

Prevent Duty

Prevent Duty Guidance

Ofsted Standards

Ofsted Safeguarding Expectations

Local Authority

Local Authority Provider Standards

25. Contact Information & Version Control

Policy Lead

Ellen Kerr

Managing Director & Designated Safeguarding Lead
(DSL), Reconnect Learning
Email: info@reconnectlearning.co.uk

Approval Details

Approved By: **Ellen Kerr**
Date Approved: **September 2026**
Effective Date: **September 2026**
Review Date: **September 2027**

Version Control

Version	Date	Author	Changes
1.0	September 2026	Ellen Kerr	Initial Issue

- ✔ This policy is current and has been developed with regard to the relevant legislation, statutory guidance and governance expectations applicable at the date of approval. Next review due September 2027.