Thriveology Wellness CIC

Online Safety Policy.

September 2026

ONLINE SAFETY POLICY

Updated for KCSIE September 2026

September 2026

INTRODUCTION

The purpose of this Online Safety Policy is to provide a framework for the safe, responsible, and legally compliant use of digital technology and the internet within Thriveology Wellness CIC. This policy aims to protect children, young people, staff, and the organisation from risks associated with online activity while promoting a positive, safe, and effective learning environment.

This policy applies to all students, Post-16 learners, staff, volunteers, and visiting professionals who use digital technology and the internet as part of Thriveology's alternative provision, outreach programme, and workplace/life-skills initiatives.
In line with **Keeping Children Safe in Education (KCSIE) 2026**, online safety is treated as a core safeguarding responsibility and is embedded across all aspects of Thriveology's practice.

OBJECTIVES

- Safeguard children, young people, and staff from online risks and harm.
- Provide clear guidelines for safe use of digital technologies and online platforms.
- Promote digital literacy, critical thinking, and responsible online behaviour.
- Ensure compliance with KCSIE 2026, UK GDPR, the Data Protection Act 2018, and relevant online-safety legislation.
- Support Post-16 learners to navigate workplace digital systems safely and appropriately.

ONLINE SAFETY PRINCIPLES

Safe and Responsible Use

All users must understand and adhere to safe practices when using the internet and digital devices to avoid risks such as cyberbullying, online grooming, exposure to harmful content, misinformation, and online radicalisation. (Original reference: "Safe and Responsible Use: All users must understand and adhere to safe practices…")

Digital Citizenship

Students and staff will be educated about respectful online behaviour, privacy settings, digital footprints, copyright, and the long-term impact of online actions.

Privacy and Data Protection

All users must comply with Thriveology's Data Protection Policy and UK GDPR. Personal information must not be shared without consent, and users must understand the risks of sharing data online. (Original reference: "All users must respect the privacy of others and comply with data protection regulations.")

Filtering, Monitoring & Security (KCSIE 2026 Requirement)

Thriveology will ensure:

- Age-appropriate filtering and monitoring systems
- Alerts for concerning online behaviour
- Secure device management
- Regular review of filtering effectiveness
- Clear escalation routes for online-safety concerns

Monitoring and Reporting

Thriveology reserves the right to monitor internet usage and digital activities on organisational devices and networks. Users must report concerns such as cyberbullying, harmful content, online exploitation, or suspicious behaviour. (Original reference: "Thriveology reserves the right to monitor internet usage…")

ARTIFICIAL INTELLIGENCE (AI) AND ONLINE SAFETY

In line with **(KCSIE) 2026**, Thriveology Wellness CIC recognises that artificial intelligence (AI), including generative AI technologies, is becoming increasingly accessible to children and young people and forms part of the wider online safety landscape. AI presents valuable opportunities for learning, creativity and accessibility; however, it also introduces emerging safeguarding risks that must be understood and managed appropriately.

Thriveology acknowledges that AI can influence all four areas of online risk identified within KCSIE 2026:

- **Content Risk** – exposure to inappropriate, harmful, misleading, extremist, sexualised, discriminatory or AI-generated content.
- **Contact Risk** – harmful interactions with other users or AI systems that simulate human interaction, including grooming, manipulation, exploitation or coercion.
- **Conduct Risk** – misuse of AI by individuals to create, share or distribute harmful content, cyberbullying, harassment or abuse.

- **Commerce Risk** – financial scams, phishing, fraud, misinformation and deceptive online practices facilitated by AI technology.

Potential AI-Related Safeguarding Risks

Children and young people may be exposed to, or engage in, unsafe use of AI technologies, including:

- Creation or sharing of AI-generated sexualised, nude or semi-nude images.
- Deepfake images, videos or audio recordings designed to humiliate, harass, manipulate or exploit others.
- AI-generated cyberbullying, harassment, intimidation or discrimination.
- False information, misinformation and disinformation created through AI tools.
- AI-generated content promoting self-harm, suicide, eating disorders, radicalisation or harmful behaviours.
- Impersonation of pupils, staff or other individuals through AI-generated text, images, audio or video.
- Use of AI tools to facilitate child-on-child abuse, coercion, exploitation or grooming.
- Excessive reliance on AI that affects critical thinking, decision-making or safe online judgement.
- Exposure to inaccurate, biased, unsafe or age-inappropriate information generated by AI systems.

Education and Awareness

Thriveology will support children, young people, Post-16 learners, staff and parents to develop an age-appropriate understanding of AI by:

- Teaching safe, responsible and ethical use of AI technologies.
- Developing critical thinking skills when evaluating AI-generated content.
- Promoting awareness that AI-generated information may not always be accurate, reliable or unbiased.
- Encouraging learners to verify information from trusted sources.
- Supporting understanding of consent, privacy and the implications of sharing content generated through AI tools.
- Raising awareness of deepfakes, manipulated media and online deception.
- Explaining the potential legal, safeguarding and wellbeing consequences of misusing AI technologies.

Staff Responsibilities in Relation to AI

Staff will:

- Maintain awareness of emerging AI technologies and associated safeguarding risks.
- Monitor the use of AI tools within educational and support activities.
- Challenge and report any misuse of AI that may place children, young people or staff at risk.

- Ensure concerns relating to AI-generated abuse, exploitation, sexualised imagery, bullying or harmful content are reported immediately to the Designated Safeguarding Lead (DSL).
- Consider AI-related risks when completing online safety, safeguarding and digital risk assessments.
- Follow organisational guidance regarding the safe and responsible use of AI technologies,

AI Misuse and Safeguarding Concerns

Any misuse of AI technology that causes harm, distress, exploitation, harassment, discrimination or risk to a child or young person will be treated as a safeguarding concern. Where AI-generated content forms part of an incident, Thriveology will:

- Preserve digital evidence where appropriate.
- Assess risks to all individuals involved.
- Follow safeguarding and child protection procedures.
- Complete and review risk assessments.
- Refer concerns to external agencies, including police or children's social care, where appropriate.
- Provide support for victims and appropriate intervention for those responsible for harmful behaviour.

AI, Filtering and Monitoring

In accordance with KCSIE 2026 expectations regarding filtering and monitoring, Thriveology will regularly review emerging AI technologies and associated risks to ensure that safeguarding systems, monitoring arrangements and staff knowledge remain effective and appropriate. AI-related concerns identified through filtering and monitoring systems will be managed through existing safeguarding procedures.

RESPONSIBILITIES

Staff Responsibilities

- **Training:** Staff must complete annual online-safety and digital safeguarding training.
- **Supervision:** Staff will monitor students' online activities and provide guidance on safe use.
- **Reporting:** Staff must report online-safety concerns to the Designated Safeguarding Lead (DSL) immediately.
- **Modelling:** Staff must model safe, respectful, and appropriate online behaviour.
- **Curriculum Delivery:** Staff must embed online safety into teaching, mentoring, outreach, and Post-16 sessions.

Student Responsibilities

- Treat others respectfully online.
- Follow safe-use guidelines and organisational rules.
- Report cyberbullying, harmful content, or unsafe behaviour.
- Understand the impact of digital footprints. (Original reference: “Students are expected to treat others with respect online…”)

Post-16 Learner Responsibilities

- Use workplace digital systems safely and appropriately.
- Follow employer digital-safety rules and Thriveology guidance.
- Report concerns relating to workplace technology, communication platforms, or digital conduct.

Parent/Guardian Responsibilities

- Engage in conversations about online safety at home.
- Monitor their child’s online activity.
- Report concerns to Thriveology promptly. (Original reference: “Parents should monitor their children's online activities…”)

ONLINE SAFETY EDUCATION

Thriveology will provide regular online-safety education for students, Post-16 learners, staff, and parents, covering:

- Online risks (cyberbullying, grooming, radicalisation, scams, misinformation).
- Protecting personal information and privacy.
- Safe use of social media, messaging apps, and online communities.
- Identifying and reporting harmful or illegal content.
- Understanding digital footprints and long-term implications.
- Safe use of workplace digital systems for Post-16 learners. (Original reference: “Thriveology will provide regular online safety education…”)

SAFE USE OF TECHNOLOGY IN ALTERNATIVE PROVISION & OUTREACH

- Devices used in AP sessions will be supervised and monitored.
- Outreach staff will support schools with online-safety strategies and interventions.
- Risk assessments will be completed for digital activities involving vulnerable learners.
- Online communication with students will follow safeguarding protocols.

SAFE USE OF TECHNOLOGY IN POST-16 WORKPLACE & LIFE-SKILLS PROGRAMMES

Post-16 learners will receive guidance on:

- Safe use of workplace email, communication platforms, and digital tools.
- Professional digital conduct and boundaries.
- Avoiding online scams, phishing, and unsafe downloads.
- Managing online presence when applying for jobs.
- Understanding employer digital-safety policies.

INCIDENT RESPONSE

In the event of an online-safety incident:

1. **Immediate Action:** Address any immediate threats to safety or wellbeing.
2. **Reporting:** Report the incident to the DSL or Deputy DSL.
3. **Investigation:** Conduct a thorough investigation, including digital evidence review.
4. **Support:** Provide support to affected individuals, including counselling if needed.
5. **External Referral:** Refer to police, social care, or external agencies where required under KCSIE.
6. **Review:** Identify lessons learned and update practice accordingly. (Original reference: “Immediate Action… Reporting… Investigation… Support…”)

ONLINE COMMUNICATION & SOCIAL MEDIA

- Staff must not communicate with students via personal accounts.
- Professional boundaries must be maintained at all times.
- Thriveology’s social media will be managed by authorised staff only.
- Images or videos of students will not be shared without consent.

REMOTE LEARNING & DIGITAL CONTACT

Where remote learning or digital communication is used:

- Sessions must follow safeguarding protocols.
- Staff must use approved platforms only.
- Students must behave respectfully and safely online.
- Parents should be informed of remote-learning arrangements.

ACKNOWLEDGMENT

By using Thriveology’s digital resources, all students, staff, Post-16 learners, and parents acknowledge that they have read, understood, and agree to comply with this Online Safety Policy. (Original reference: “By using Thriveology's digital resources…”)

REVIEW AND UPDATES

This Online Safety Policy will be reviewed annually or sooner if required by:

- Changes in KCSIE
- Emerging online risks
- Technological developments
- Safeguarding updates
- Organisational changes

Review Date: **September 2027**