E-Safety / Online Safety Policy

Thrive Alternative Provision

Date applied: September 2025
Review date: September 2026
Policy lead: Jack Broadhead (Managing Director)

1. Purpose

Thrive Alternative Provision aims to ensure that all members of the school community — pupils, staff, governors and visitors — use technology safely and responsibly. This policy:

- Protects all users from online harms, including inappropriate content, cyberbullying, exploitation, radicalisation and illegal activity.
- Defines roles and responsibilities for online safety.
- Sets out expectations for acceptable online behaviour.
- Ensures appropriate filtering, monitoring, and safeguarding systems are in place.
- Supports pupils to develop knowledge and skills to navigate digital environments safely.

This policy applies to all technology used on or off site, including school-owned and personal devices where Thrive has responsibilities for supervision.

2. Statutory and Local Framework

Online safety is part of statutory safeguarding duties under **Keeping Children Safe in Education (KCSIE, 2025)**, which states settings must protect pupils from harmful online material and have appropriate filters and monitoring systems.

Thrive also complies with relevant UK legislative requirements such as the **Online Safety Act 2023**, data protection law, and any applicable local authority expectations.

3. Roles and Responsibilities

3.1 Governing Body / Proprietor

- Ensures a robust online safety policy is in place.
- Approves the policy and monitors its implementation.
- Ensures adequate resources for online safety provision.

3.2 Designated Safeguarding Lead (DSL)

- Leads on online safety as part of overall safeguarding arrangements.
- Reports online safety concerns promptly via safeguarding procedures.
- Liaises with IT support to ensure filtering and monitoring are effective.

3.3 Staff

- Understand and implement this policy.
- Supervise and guide pupils in safe online use.
- Report concerns regarding safeguarding procedures.

3.4 Pupils

- Follow the acceptable use rules and report concerns to a trusted adult.

3.5 Parents/Carers

- Support safe online behaviours at home.
- Work with Thrive to address concerns about online activity.

4. Acceptable Use of Technology

Staff

Staff must use technology responsibly and professionally, including email, internet, and social media:

- Only use approved platforms for communication with pupils.
- Maintain professional boundaries online.
- Avoid sharing personal contact details with pupils.

Pupils

Pupils are expected to:

- Use technology responsibly and respectfully.
- Not attempt to bypass filtering or monitoring systems.
- Report any harmful or inappropriate content or contact to staff.

Parents/Carers

We ask parents/carers to support Thrive's online safety standards at home and communicate any concerns.

5. Filtering, Monitoring and Technical Safeguards

Thrive will:

- Provide appropriate filtering and monitoring to block harmful or inappropriate content on all school-managed networks and devices.
- Work with IT support providers to ensure systems are reviewed regularly.
- Balance safeguarding needs with educational access to digital tools.

Settings must ensure that systems are appropriate and proportionate. Filtering and monitoring should protect users from content such as adult material, hate speech, illegal activity, self-harm advocacy, and exploitation.

6. Education and Training

For Pupils

Online safety education is embedded within the curriculum and includes:

- How to use the internet safely, responsibly, and respectfully.
- Risks including cyberbullying, grooming, radicalisation, scams, and misinformation.
- Where to go for help and how to report concerns.

For Staff

Staff receive ongoing training to:

- Recognise online safety risks and respond appropriately.
- Use reporting tools and safeguarding systems effectively.
- Stay updated with emerging online risks.

Training is part of safeguarding updates and induction processes.

7. Managing Online Safety Incidents

Online safety concerns should be responded to promptly and appropriately, following Thrive's **Safeguarding and Child Protection Policy**. This includes:

- Recording incidents accurately in the safeguarding system.
- Following escalation procedures for serious incidents.
- Providing support and education to pupils involved.

Examples of concerns include:

- Viewing or sharing harmful content
- Cyberbullying
- Grooming or harmful contact attempts
- Sexting
- Online harassment
- Exposure to extremist content

Where required, incidents will be reported to external agencies, including the police.

8. Use of Personal Devices and Social Media

- Personal devices may be used under supervised arrangements if appropriate (e.g., for learning).
- Pupils must follow the acceptable use standards whether on school-owned or personal devices.
- Staff should not communicate with pupils via personal social media or private accounts.

9. Remote Learning and Off-Site Online Safety

When communicating or teaching online:

- Approved platforms and channels must be used.
- Staff and pupils must follow the same behaviour and safeguarding standards as in person.
- Parents should supervise younger pupils' remote activity.

Remote learning guidelines should be clear and shared in advance.

10. Policy Review and Updates

This policy will be reviewed at least **annually** or sooner in response to significant changes in:

- Technology
- Legislation
- National or local guidance
- Incidents and trends identified in Thrive

The review should include input from staff, governors and, where appropriate, pupils and parents.

11. Links to Other Policies

Thrive's e-Safety Policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Acceptable Use Agreements for Staff and Pupils
- Data Protection Policy
- Mobile Phone / Device Policy

12. Sign-Off

Signed (Head/Director): Jack Broadhead
Date: 02/09/2025
Review date:02/09/2026