

# Flip The Script YOUTH CIC

## ONLINE SAFETY POLICY

Document:	ONLINE SAFETY POLICY
Owner:	Lylas Flora & Kyra Palma, Directors & DSL
Date:	January 2026

### 1. PURPOSE

This policy outlines how Flip The Script Youth CIC protects children and young people online and teaches them to protect themselves. Online safety is an essential part of safeguarding and encompasses all digital interactions.

### 2. SCOPE

This policy covers:

- Use of technology in our premises
- Online communications with young people
- Digital content creation and sharing
- Online youth work and virtual sessions
- Social media presence

### 3. ONLINE RISKS

Young people face online risks including:

- Content: exposure to illegal, harmful, or age-inappropriate content
- Contact: harmful online interaction with others
- Conduct: personal online behaviour that increases risk
- Commerce: online fraud, gambling, phishing

Specific concerns include:

Page 1 of 4



- Cyberbullying and online harassment
- Online grooming and sexual exploitation
- Radicalisation
- Exposure to violent or harmful content
- Sharing of nude/semi-nude images
- Online gambling or financial scams
- Impact on mental health and wellbeing

## 4. STAFF RESPONSIBILITIES

All staff must:

- Be aware of online safety risks
- Report concerns about online activity immediately
- Follow this policy when using technology with young people
- Model safe online behaviour
- Never share personal social media accounts with young people
- Only contact young people through official channels

## 5. ACCEPTABLE USE

Technology in our premises must:

- Be used for appropriate purposes only
- Have appropriate filtering and monitoring
- Not be used to access inappropriate content
- Be used in visible areas where possible

## 6. ONLINE COMMUNICATIONS

When communicating online with young people:

- Use official organisational accounts only
- Maintain professional boundaries



- Keep communications transparent (copy in colleagues where appropriate)
- Respond during working hours where possible
- Never arrange to meet young people privately
- Save records of communications

## 7. VIRTUAL SESSIONS

When delivering online sessions:

- Use secure platforms with appropriate controls
- Ensure two staff members are present
- Keep cameras on and sessions recorded where appropriate
- Set clear ground rules with young people
- Have an emergency plan for safeguarding concerns

## 8. SOCIAL MEDIA

Official social media accounts must:

- Have clear terms of use
- Be managed by designated staff
- Not accept friend requests from young people on organisational accounts
- Moderate comments and remove inappropriate content
- Never share images of young people without consent

## 9. EDUCATION

We will teach young people about:

- How to stay safe online
- Privacy settings and data protection
- Recognising and reporting online abuse
- The permanence of digital footprints
- Healthy relationships online



- Critical thinking about online content

## 10. RESPONDING TO CONCERNS

If you become aware of online harm:

- Follow safeguarding procedures immediately
- Do not investigate further or view illegal content
- Preserve evidence where possible (screenshots, etc.)
- Report to DSL who will decide on referral to police/social care
- Consider whether other young people may be at risk

