Digital Safeguarding Policy

Part of the BYO Media and Communications Policy Suite

CONTENTS

Document Details	Information
Policy Title	Digital Safeguarding Policy
Version	3.0
Effective Date	24 June 2025
Review Date	24 June 2027
Owner	Designated Safeguarding Lead
Approved By	Hassan Kingsley, Governor
Cross-References	Safeguarding Policy Framework, Child Protection Procedures, Adult Safeguarding Procedures, Data Protection Policy, Anti-Bullying Policy, Code of Conduct Policy, Whistleblowing Policy

1. Policy Statement

This policy covers how we stay safe online and use digital technology responsibly at BYO. It's about keeping everyone safe while still being able to share the great work we do and connect with our community.

This policy covers:

- Taking photos and videos
- Social media use
- Online communication
- Digital devices and technology
- Staying safe online
- Data protection in digital contexts

Applies to: All staff, volunteers, young people, and anyone representing BYO online.

Safeguarding Integration: This policy is part of our comprehensive **Safeguarding Policy Framework** and should be read alongside our **Child Protection Procedures** and **Adult Safeguarding Procedures**.

Data Protection: All digital activities must comply with our **Data Protection Policy** regarding collection, storage, and sharing of personal information.

2. The Basics - Keep It Simple

Golden Rules:

- **Think before you post** - would you be happy for anyone to see it?
- **Get permission** before taking photos/videos of people
- **Keep it positive** - represent BYO well online
- **Report concerns** - if something doesn't feel right, tell someone
- **Respect privacy** - not everything needs to be shared online
- **Follow safeguarding principles** - online and offline safety are connected

Code of Conduct: These digital expectations align with our **Code of Conduct Policy** for staff and volunteers and **Code of Behaviour Policy** for young people.

3. Photography and Video

3.1 Taking Photos and Videos

Permission:

- General consent is covered in our registration forms
- For specific individual photos, ask first
- Respect if someone says no
- Parents/guardians can withdraw consent anytime
- Special considerations for vulnerable adults who may lack capacity

What's OK:

- Group photos of activities and events
- Action shots during sports/activities
- Close-up shots of individuals with specific permission or where general consent applies
- Photos showing BYO's work, impact, and community spirit
- Celebrating achievements and personal milestones (with appropriate consent)

What's Not OK:

- Close-up individual photos without appropriate consent
- Images that could embarrass, endanger, or compromise someone's dignity
- Photos in changing areas, toilets, or other private spaces
- Taking photos for personal use of other people's children
- Images that could reasonably be misused or exploited (e.g. suggestive poses, vulnerable situations)

3.2 Using Photos and Videos

We can use images for:

- BYO social media accounts
- Website and promotional materials
- Funding applications and reports
- Local media and press coverage
- Internal training and evaluation

Good practice:

- Focus on activities, but don't avoid close-ups where there is consent
- Use general descriptions (e.g. "BYO workshop") unless specific context enhances the story and permission allows
- Name individuals only with specific permission or where general consent covers it and it's non-sensitive
- Remove images promptly if someone requests it
- Always consider safeguarding risks — avoid sharing anything that could embarrass, compromise dignity, or be misused

Data Protection: Image storage and sharing must comply with our **Data Protection Policy** regarding consent, retention, and security.

3.3 Storage and Security

Keep it secure:

- Store images on BYO approved systems only
- Don't keep unnecessary copies on personal devices
- Delete images when no longer needed according to retention schedule
- Backup important images securely
- Report lost devices containing images immediately

4. Social Media

4.1 BYO Official Accounts

Who can use them:

- Only designated staff/volunteers with login details
- Don't share passwords or login details
- Check with DSL before setting up new accounts
- All users must be appropriately vetted through our Recruitment, Selection and Onboarding Policy

What to post:

- Positive stories about BYO activities
- Achievements and celebrations
- Information about upcoming events
- Community engagement content
- Safeguarding-appropriate content only

4.2 Personal Social Media

If you mention BYO on personal accounts:

- Remember you're representing us as outlined in our Code of Conduct Policy
- Keep it positive and professional
- Don't share confidential information
- Think about how it reflects on BYO
- Consider data protection implications

Staff and volunteer guidance:

- Don't friend/follow young people on personal accounts (unless family/pre-existing relationship)
- Keep personal and professional boundaries clear
- Be mindful of privacy settings
- Consider who can see your posts
- Report concerns about online interactions with young people

4.3 Young People's Social Media

What we do:

- Educate about online safety and digital citizenship
- Monitor BYO-related content for safeguarding concerns
- Support young people who experience online issues
- Encourage positive online behaviour as outlined in our Code of Behaviour Policy

What we don't do:

- Monitor personal accounts (that's for parents/carers)
- Friend/follow young people on official BYO accounts
- Share personal information about young people

Bullying: Online bullying is addressed through our Anti-Bullying Policy and may trigger safeguarding procedures.

5. Online Communication

5.1 Communicating with Young People

Best practice:

- Use BYO official channels where possible
- Keep communications professional and transparent
- Include parents/carers in communications with under 16s
- Avoid private messaging with young people
- Follow safeguarding principles for all communication

Acceptable:

- Group communications about BYO activities
- Public comments on BYO social media posts
- Official emails with parents copied in
- Emergency communications through official channels

Not acceptable:

- Private messaging individual young people
- Sharing personal contact details
- Late-night communications
- Personal conversations unrelated to BYO activities
- Any communication that could be seen as grooming

Safeguarding: Any concerning online communication must be reported to our DSL following Child Protection Procedures.

5.2 Digital Devices at Activities

Staff/volunteer devices:

- Can be used for BYO purposes (photos, emergency contact)
- Keep personal use to minimum during activities
- Secure devices and don't leave unattended
- Young people shouldn't have access to staff personal devices
- Report lost or stolen devices immediately

Young people's devices:

- Can generally use their own devices during appropriate times
- Encourage responsible use as per Code of Behaviour Policy
- Address inappropriate use through normal behaviour management
- Parents/carers responsible for their child's device use

6. Online Safety Education

6.1 What We Teach Young People

Digital citizenship:

- How to behave respectfully online
- Understanding privacy settings and digital footprints
- Recognizing and reporting online risks
- Critical thinking about online content
- Connections between online and offline behaviour

Staying safe online:

- Not sharing personal information with strangers
- Understanding that not everyone online is who they say they are
- What to do if they see something that makes them uncomfortable
- How to report concerns and get help
- Recognizing grooming and exploitation risks

6.2 Supporting Parents/Carers

We provide:

- Information about online safety
- Guidance on age-appropriate technology use
- Signposting to additional resources
- Support when online safety concerns arise
- Connection to our broader safeguarding framework

7. Recognizing and Responding to Concerns

7.1 What to Look Out For

Online safety concerns:

- Young people sharing too much personal information
- Inappropriate contact from strangers
- Cyberbullying or online harassment
- Exposure to inappropriate content
- Signs of online grooming or exploitation
- Adults attempting to isolate young people online

Digital behaviour concerns:

- Excessive screen time affecting participation
- Using technology to harm or exclude others
- Sharing inappropriate content
- Inappropriate online relationships
- Signs of exploitation or abuse through digital means

Bullying: Online bullying incidents should be addressed through our **Anti-Bullying Policy** and may escalate to safeguarding procedures.

7.2 How to Respond

If you're concerned:

1. **Don't investigate yourself** - you might compromise evidence
2. **Report to DSL immediately** - Joshua William Hall (07925 328 728)
3. **Support the young person** - reassure them they're not in trouble
4. **Document concerns** - date, time, what you observed
5. **Follow normal safeguarding procedures** as outlined in **Child Protection Procedures**

For less serious issues:

- Address through normal behaviour management per Code of Behaviour Policy
- Educate about appropriate online behaviour
- Involve parents/carers as appropriate
- Monitor and support ongoing

Alternative Reporting: If you feel unable to report through normal channels, see our **Whistleblowing Policy** for alternative options.

8. Data Protection and Privacy

8.1 Personal Information Online

Be careful with:

- Names, addresses, and contact details
- Images that could identify individuals
- Personal circumstances and information
- Medical or family information
- Any information that could be used to harm or exploit

Good practice:

- Only collect information you need
- Store it securely and don't share unnecessarily
- Delete when no longer needed
- Check you have permission to use/share information
- Follow data minimization principles

Data Protection: All handling of personal information must comply with our **Data Protection Policy.**

8.2 Digital Records and Security

Keep secure:

- Use strong passwords and change them regularly
- Don't save passwords on shared computers
- Log out of accounts when finished
- Report lost devices or security concerns immediately
- Use two-factor authentication where available

9. Incident Management

9.1 Types of Incidents

Safeguarding incidents:

- Online grooming or inappropriate contact
- Cyberbullying involving BYO participants
- Exposure to harmful content
- Sharing of inappropriate images
- Digital exploitation or abuse

Reputation incidents:

- Negative posts about BYO
- Inappropriate content associated with BYO
- Misinformation or rumours online
- Privacy breaches

9.2 Response Process

Immediate action:

1. **Ensure safety** - is anyone at immediate risk?
2. **Report to DSL** - for safeguarding concerns
3. **Document everything** - screenshots, details, timeline
4. **Don't engage publicly** - avoid online arguments or debates
5. **Seek advice** - from DSL or external agencies
6. **Consider police involvement** - for criminal activity

Follow-up:

- Support affected individuals
- Review what happened and learn from it
- Update procedures if needed
- Communicate with community if appropriate
- Report to relevant authorities as required

Serious Incidents: Major incidents may require procedures outlined in **Managing Allegations about Staff and Volunteers** or external agency involvement.

10. Key Contacts and Support

10.1 Internal Support

Designated Safeguarding Lead (DSL): Joshua William Hall

- Mobile: 07925 328 728
- Email: joshuahall@britanniayo.com

Deputy DSL: Hassan Alexander Kingsley

- Mobile: 07597 874 222
- Email: hassankingsley@britanniayo.com

Main Office: 0121 448 7378

10.2 External Resources

For reporting concerns:

- **CEOP**: Report online child sexual abuse and exploitation
- **Internet Watch Foundation**: Report criminal online content
- **Action Fraud**: Report online fraud and cybercrime
- **Police**: 999 for emergencies, 101 for non-emergencies

For support and guidance:

- **Childnet**: Online safety resources and advice
- **UK Safer Internet Centre**: Safety tips and resources
- **NSPCC**: Online safety guidance - 0808 800 5000
- **Professional Online Safety Helpline**: 0344 381 4772

10.3 For Young People and Parents

Immediate support:

- **Childline**: 0800 1111 (free, confidential support)
- **Report Remove**: Tool for removing inappropriate images
- **Think U Know**: Online safety education for different ages
- **Samaritans**: 116 123 (free 24/7 emotional support)

11. Training and Development

11.1 Staff and Volunteer Training

Basic requirements:

- Understanding of this policy
- Basic online safety awareness
- How to report concerns through **Child Protection Procedures**
- Appropriate use of social media and photography
- Data protection responsibilities

Ongoing development:

- Updates on new technologies and risks
- Sharing experiences and good practice
- External training opportunities where available
- Integration with broader safeguarding training

Training Framework: Digital safeguarding training is integrated with our **Safeguarding Policy Framework** training requirements.

11.2 Young People's Education

Integrated into activities:

- Online safety conversations during regular activities
- Practical examples and scenarios
- Peer-to-peer learning and support
- Celebrating positive online behaviour
- Connection to offline safety principles

12. Related Policies

This policy works with:

- **Safeguarding Policy Framework**
- **Child Protection Procedures**
- **Adult Safeguarding Procedures**
- **Data Protection Policy**
- **Photography and Videography Policy**
- **Social Media Policy**
- **Anti-Bullying Policy**
- **Code of Conduct Policy**
- **Code of Behaviour Policy**
- **Whistleblowing Policy**
- **Managing Allegations about Staff and Volunteers**

13. Policy Review and Updates

This policy will be reviewed annually and updated as technology changes. We'll learn from experiences and keep improving our approach to digital safeguarding.

Key principles remain constant:

- Technology changes fast, but the principles of keeping people safe, treating others with respect, and using common sense remain the same
- Online and offline safeguarding are interconnected
- Prevention through education is key
- Swift response to concerns protects everyone

Quick Reference Summary

Keep it simple: Think before you share, get permission for photos, and report concerns. When in doubt, ask for advice.

Remember:

- All digital activity connects to our safeguarding responsibilities
- Data protection and privacy matter online
- Young people need education and support, not monitoring
- Staff and volunteers must maintain professional boundaries online
- Report all concerns through proper channels

Document Control:

- This policy forms part of BYO's comprehensive safeguarding framework
- All staff receive training on digital safeguarding as part of broader safeguarding training
- Regular reviews ensure the policy remains current with technological developments

Reviewed by:

Hassan Kingsley
Date: 24/06/2025
Next Review Date: 24/06/2027

This policy forms part of BYO's commitment to safeguarding and should be read alongside our complete Safeguarding Framework.

Britannia Youth Organisation CIC is a Community Interest Company registered in England and Wales. Company No. 12515346 | Registered Address: 36 St Joseph's Rd, Ward End, Birmingham, B8 2JU