E-Safety Policy

Policy Details	
Date Review	March 2025
Date of next review	March 2026

This policy outlines the approach Y.O.U.R Beauty School takes to ensure that students, staff and stakeholders are protected and educated in their use of digital technologies. It is aligned with the latest UK statutory guidance, including *Keeping Children Safe in Education* (KCSIE), the *Prevent* Strategy, the Ofsted Inspection Framework, and *Working Together to Safeguard Children*. This document should be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Data Protection Policy and Acceptable Use Agreements (AUA).

---

1. Aims and Scope

Y.O.U.R Beauty School recognises the central role that digital technologies play in modern life and education. We are committed to supporting all students and staff in using technology in a safe, responsible and informed way. This policy applies to all members of the school community: students (including post-16 learners), staff, volunteers and parents/carers.

---

2. Education and Digital Literacy

Students are taught how to:

- Stay safe online and use technology responsibly.
- Evaluate online content for accuracy, credibility and bias.
- Understand the importance of protecting their privacy and digital footprint.
- Report inappropriate or harmful content, contact or conduct.

E-safety is embedded within PSHE, RSE, Computing and vocational subject areas and delivered through assemblies, workshops and curriculum activities.

Parents and carers are supported through workshops, newsletters and signposting to trusted resources.

---

3. Key E-Safety Risks

The school educates students about the following key online safety risks:

- **Content**: Exposure to inappropriate, harmful or misleading material such as pornography, extremist content, hate speech, pro-self-harm websites and fake news.
- **Contact**: Risks posed by online grooming, cyberbullying, scams and harmful peer interaction.
- **Conduct**: Students' own behaviours, including sharing personal data or intimate images, accessing age-inappropriate content, digital addiction and copyright infringement.

Students also learn about emerging risks including AI-generated content, incel ideologies, financial scams and anonymous online apps.

---

4. Use of School Internet and Devices

- The school provides filtered and monitored internet access appropriate to students' age and maturity.
- Students are taught the acceptable use of the internet and devices and are required to sign a Student Acceptable Use Agreement.
- Staff are required to read and sign a Staff Acceptable Use Agreement before accessing ICT systems.
- Personal use of the internet by staff is not permitted during contact time and must always comply with the Adult Behaviour Policy.

---

5. Filtering and Monitoring

We have robust filtering and monitoring systems in place to:

- Prevent access to illegal or inappropriate content.
- Detect and respond to potentially harmful behaviour or activity.

Filtering and monitoring arrangements are reviewed regularly by the Leadership Team.

---

6. Social Media and Communication

Students are not permitted to access social networking sites in school.

Staff, governors, parents and carers must:

- Not disclose confidential school information or breach data protection.
- Not engage in public criticism of the school, staff, students or parents.
- Not connect with current students via social media.

- Set appropriate privacy settings on all social accounts.
- Refer any school-related grievance through official procedures, not social media.

---

7. Publishing Images and Work

- Images of students will only be published with parent/carer consent.
- Full names will not be used in school publicity materials.
- Students' work will only be published with consent.

---

8. Cyberbullying

Cyberbullying is treated with the same seriousness as other forms of bullying. It may involve text messages, social media posts, photos, videos or email harassment. All incidents will be managed in accordance with the Anti-Bullying and Behaviour Policies. Serious breaches may involve the police and external agencies.

---

9. Data Protection and Personal Information

All staff, students and stakeholders must handle personal data in accordance with the UK GDPR and Data Protection Act. Personal and sensitive data must:

- Be stored securely.
- Only be shared on a need-to-know basis.
- Not be disclosed online without proper consent.

---

10. Reporting and Handling Incidents

- All staff must report any e-safety concern or breach to the Designated Safeguarding Lead (DSL) or Head of School.
- All students will be taught how to report online concerns confidentially.
- Concerns related to child protection will be dealt with in accordance with the Safeguarding Policy.

The school maintains a risk register for e-safety issues and logs incidents and patterns to improve practice.

---

11. Training and Responsibilities

- All staff receive annual e-safety training.
- Online safety is part of staff induction and ongoing Continuing Professional Development (CPD).
- The DSL takes lead responsibility for online safety, supported by the senior leadership team.
- The Governing Body is responsible for ensuring e-safety is embedded in safeguarding practices.

---

12. Policy Review and Evaluation

This policy will be reviewed annually, or earlier if necessary, to reflect changes in legislation, guidance or school practice. Input from staff, students, governors and parents will inform the review process.

---

13. Policy Communication

- **Students**: Informed during induction and lessons; Acceptable Use is reinforced regularly.
- **Staff**: Provided during induction and annual training; reinforced through briefings and updates.
- **Parents/Carers**: Access to the policy via the school website and updates shared through newsletters.

Acknowledgement

I have read and understood the E-Safety Policy and agree to comply with its terms.

Signature: _____

Name (Printed): _____

Date: _____