



Bridging Futures

Empowering every child through inclusion, opportunity and support

Digital Technology and Online Safety Policy

Version: September 2026

Review Date: September 2027

Author: Claire Galbraith, Education Director

Our Aim

At Bridging Futures, digital technology plays an important role in supporting education, therapeutic interventions and preparation for adulthood. We use laptops and online resources to enhance learning, build independence and develop the digital skills students need for further education, employment and everyday life.

As a trauma-informed provision, we recognise that technology can be both a valuable educational tool and a potential safeguarding risk. We are committed to creating a safe environment where technology is used responsibly, respectfully and confidently.

Why We Use Technology

Technology allows students to access personalised learning, complete coursework, undertake research, improve literacy and numeracy, develop digital skills and explore future career pathways. It also supports creativity, communication, confidence and independent learning.

Alongside these opportunities, students are taught how to stay safe online, identify misinformation and make informed decisions when using digital technology.

Legal Framework

This policy reflects current legislation and statutory guidance including:

- Keeping Children Safe in Education (Current Edition)
- Working Together to Safeguard Children
- UK GDPR and the Data Protection Act 2018
- Computer Misuse Act 1990
- Prevent Duty Guidance
- DfE Filtering and Monitoring Standards
- Online Safety Act 2023
- Equality Act 2010

Scope

This policy applies to all students, staff, therapists, volunteers, parents, carers, visitors and anyone using Bridging Futures technology or accessing the internet through our systems.

Responsibilities

Everyone has a responsibility to ensure technology is used safely.

Students

Students are expected to use technology for learning, follow staff instructions, treat equipment with care and communicate respectfully online. They should keep passwords secure, report anything online that makes them feel unsafe and understand that internet activity may be filtered and monitored to support safeguarding.

Staff

Staff are responsible for modelling good digital practice, supervising technology use and teaching online safety throughout the curriculum. They must also protect confidential information, comply with data protection legislation and report any safeguarding concerns in accordance with Bridging Futures procedures.

Parents and Carers

Parents and carers play an important role in promoting positive online behaviour. We encourage families to discuss online safety regularly, monitor age-appropriate technology use at home and contact Bridging Futures if they have any concerns.

Artificial Intelligence (AI)

Artificial Intelligence is becoming an increasingly important part of education and employment. Bridging Futures encourages students to use approved AI tools responsibly to support learning, develop ideas and improve understanding.

AI must never be used to complete work dishonestly, submit generated work as a student's own or create inappropriate, harmful or offensive content. Staff will teach students how to use AI ethically, safely and responsibly.

Mobile Phones

To minimise distractions and support engagement, mobile phones must be handed to a member of staff at the beginning of each session unless alternative arrangements have been agreed. Students must not use mobile data to bypass the school's filtering systems or photograph, record or film others without permission.

Technology for Learning

Technology is used to support teaching, independent learning and personal development. Students may access Microsoft 365, Oak National Academy, Corbettmaths, BBC Bitesize, BBC Newsround and other staff-approved educational resources. Additional software and websites may be introduced where they enhance learning or therapeutic outcomes.

Websites and Apps Not Permitted

Unless authorised by staff for a specific educational purpose, students must not access social media, gaming platforms, streaming services or other inappropriate websites during the school day.

This includes applications such as Snapchat, TikTok, Instagram, Discord, Roblox and YouTube, unless YouTube is being used to access teacher-approved educational content.

Staying Safe Online

Online safety forms part of everyday learning at Bridging Futures. Students are taught how to protect their personal information, communicate respectfully, recognise misinformation and report cyberbullying or any online content that makes them feel uncomfortable.

Internet filtering and monitoring systems operate across all Bridging Futures devices to support safeguarding and meet national standards.

Online Safety Education

Digital safety is embedded throughout the curriculum rather than taught as a standalone topic. Students learn about cyberbullying, healthy online relationships, misinformation, privacy, digital wellbeing, Artificial Intelligence, online exploitation and developing positive digital habits that prepare them for adult life.

Reporting Concerns

Any concerns relating to online safety, cyberbullying, inappropriate content or suspicious online behaviour should be reported immediately to a member of staff.

All reports will be taken seriously and managed in line with the Bridging Futures Safeguarding and Child Protection Policy. Where necessary, parents, carers, external agencies or the police may be involved.

Responding to Misuse

Technology is provided to support learning and should always be used responsibly. Where misuse occurs, staff will respond fairly, proportionately and with a restorative approach wherever possible.

Responses may include reminding students of expectations, providing further online safety education, temporarily removing access to technology, contacting parents or carers, applying behaviour sanctions or referring concerns to the Designated Safeguarding Lead where safeguarding issues are identified.

Related Policies

This policy should be read alongside the:

- Safeguarding and Child Protection Policy
- Behaviour and Relationships Policy
- Mobile Phone Policy
- Staff Code of Conduct
- Data Protection Policy
- SEND Policy
- Health and Safety Policy
- Complaints Policy

Policy Review

This policy will be reviewed annually, or sooner if changes to legislation or safeguarding guidance require it.

Review Date: September 2027

Author: Claire Galbraith

Education Director – Bridging Futures