E-Safety Policy

1. Introduction

Information technology and online communication provide unparalleled learning opportunities beyond traditional learning methods, but they also bring more significant and subtle risks to young people. Therefore, our students are taught how to stay safe in online environments and how to reduce risks, including but not limited to identity theft, bullying, harassment, grooming, stalking, abuse, and radicalisation.

New technologies continuously enhance communication, information sharing, learning, social interaction, and leisure activities. Current and emerging technologies used both in and out of school may include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Artificial intelligence (AI);
- Metaverse;
- Music/video downloads;
- Gaming websites;
- Text and picture messages;
- Video calls;
- Podcasts;
- Online communities via gaming consoles;
- Mobile internet devices such as smartphones and tablets.

The implementation of this policy aims to protect the interests and safety of the entire BBEVA community. It provides clear guidance on minimising risks and handling policy violations.

At BBEVA, we are committed to maintaining E-Safety for staff and students and classify potential E-Safety issues into four risk areas:

- Content: Exposure to illegal, inappropriate, or harmful content, e.g., pornography, fake news, racism, sexism, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- Contact: Harmful online interactions with other users, e.g., peer pressure, commercial advertising, adults impersonating children or young adults to groom or exploit them for sexual, criminal, financial, or other purposes.
- Conduct: Online behaviour that increases the likelihood of harm or causes harm, e.g.,

sending, receiving, or producing pornographic images (including voluntary/non-voluntary sharing of nude/semi-nude photos and/or explicit content), sharing other explicit images, and online bullying.

• Commerce: Risks such as online gambling, inappropriate advertising, phishing, and/or financial fraud.

We recognise the responsibility to educate students about E-Safety, teach appropriate behaviour and critical thinking skills, and ensure they remain safe and law-abiding when using the internet and related technologies, both in and out of class. We also acknowledge the importance of involving students in E-Safety discussions and listening to their concerns, anxieties, thoughts, and suggestions.

This policy applies to all BBEVA community members, including staff, students, parents, teachers, and support staff who have access to BBEVA's IT systems and equipment.
In this policy, "Staff" includes teaching and non-teaching staff, as well as board members. "Parents" include students' guardians.

This policy applies to:

- All employees, independent contractors, volunteers, and interns of the company.
- All students enrolled in our online courses, tutoring, or educational consulting services.
- Parents/guardians of students related to our services.
- All online activities and digital communications conducted for or on behalf of the company, whether using company-provided or personal devices.
- All online platforms, software, and tools are used for teaching, learning, communication, and administrative purposes.

This policy covers fixed and mobile internet devices (e.g., PCs, laptops, cameras, tablets, interactive whiteboards, digital video equipment, etc.).

This policy document should be read alongside:

i. Behaviour and Discipline Policy
ii. Acceptable Use of Technology Policy
iii. Child Safeguarding Policy
iv. Privacy Policy

2. Roles and Responsibilities

- Board of Directors

  BBEVA's governing body is responsible for approving this policy and reviewing its effectiveness periodically. The Board reviews the policy annually. The Designated

Board member for safeguarding ensures the implementation of the E-Safety Policy.

- Head and Senior Leadership Team

  This team is responsible for approving the policy and evaluating its effectiveness, as well as being accountable for the safety of BBEVA community members, including E-Safety responsibilities. Specifically, the Head and Senior Leadership Team ensure staff receive adequate E-Safety training and understand BBEVA's procedures and policies in the event of an E-Safety breach or alleged breach.

- Designated Safeguarding Lead (DSL)

  BBEVA's DSL handles day-to-day E-Safety matters. The DSL ensures all BBEVA community members comply with this policy and collaborates with IT staff to achieve this. The DSL continuously updates knowledge on E-Safety issues and guidance from relevant organisations.

- IT Staff

  Responsible for advising on secure technical practices, recommending safe platforms, and assisting with technical aspects of E-Safety.

- Staff and Support Personnel

  All staff must sign the Acceptable Use of Technology Policy before accessing any IT system. As with all safety matters, staff are encouraged to foster an open communication culture to address any E-Safety issues that may arise. Staff must document and report any E-Safety incidents or concerns and submit records to BBEVA's DSL as soon as possible.

- Students

  Students are responsible for using BBEVA's systems per the Acceptable Use of Technology Policy and reporting misuse to staff.

- Parents and Guardians

  We believe parents and guardians are vital in promoting E-Safety both within and outside BBEVA. We regularly consult on E-Safety and strive to raise awareness of internet-related risks and benefits. If BBEVA has concerns about a student's behaviour in this area, we will contact parents/guardians, who are likewise encouraged to share concerns with BBEVA.

  Parents and guardians are responsible for supporting the Acceptable Use Agreement.

---

3. Education and Training

- Staff and Teachers: Awareness and Training

  New teachers receive E-Safety and Acceptable Use of Technology information during induction. All teaching staff regularly receive updates on E-Safety issues via internal training and meetings, and understand their safeguarding and E-Safety

responsibilities.

All staff interacting with students must demonstrate, promote, and support safe behaviours in class and adhere to BBEVA's E-Safety procedures. These are outlined in the Acceptable Use of Technology Policy, which staff must sign before using platforms.

Teachers are encouraged to integrate E-Safety activities into subjects, address emerging issues through discussion, and know how to respond to technology misuse by BBEVA community members.

Any E-Safety incident must be documented and reported to the DSL immediately. The DSL records all incidents, follows up with students/parents/staff, and monitors as needed.

- Students: E-Safety in the Curriculum

  We believe students must receive regular and meaningful E-Safety guidance. We continuously seek new opportunities to promote E-Safety and monitor students' understanding.

  BBEVA integrates E-Safety teaching across multidisciplinary curricula. Informally, students are educated on recognising technological dangers they may encounter outside BBEVA.

  Age-appropriately, students learn their responsibilities for online safety and how to protect themselves, typically through in-class and extracurricular teaching. They learn to identify online sexual exploitation, grooming, stalking, and risks, and how to report incidents affecting themselves or peers. Concerns can be reported to the DSL or any staff member (who will escalate to the DSL).

  Students also learn internet-related laws (e.g., data protection, intellectual property) and respect for others' information/images through discussions and activities.

  Students understand the impact of cyberbullying and know how to seek help. They should approach the DSL, parents/guardians, peers, or staff for advice, especially when facing internet-related issues.

- Parents and Guardians: Close Collaboration

  BBEVA works closely with parents/guardians to promote an E-Safety culture. BBEVA contacts parents/guardians regarding concerns about student behaviour, and vice versa.

  BBEVA recognises that not all parents/guardians feel equipped to protect children's device use at home and encourages them to seek help via our customer support team.

---

4. Use of Devices

- **Use of Personal Devices**

  While we acknowledge staff and teachers may use personal devices, the following rules are mandatory:

  - Security: All personal devices used for company activities must have an updated OS, antivirus/anti-malware, and strong passwords/biometric security.
  - Privacy: Users must ensure personal data on devices does not expose company or student data. Work-related activities should be separated from personal use where possible.
  - Data Protection: Sensitive company/student data must not be stored on personal devices unless encrypted and handled securely per company data protection guidelines.
  - Company Software: Only company-approved software/platforms may be used for official communication/teaching.
  - Incident Response: Suspected security breaches/E-Safety incidents involving personal devices must be reported immediately to the DSL and IT support.

- **Online Platforms and Communication**

  - Approved Platforms Only: All teaching, tutoring, consulting, and official communication with students/parents must occur via company-approved secure platforms (e.g., specific video conferencing software).
  - Professional Conduct: Staff and teachers must maintain professional and respectful communication at all times. Inappropriate language/content/behaviour is prohibited.
  - Private Communication: Private/unmonitored communication with students/parents/guardians outside approved platforms is forbidden (includes personal messaging apps, social media DMs, or private emails).
  - Session Recording: Online lessons/tutoring may be recorded (with prior notice/consent) for safeguarding, quality assurance, and review. Recordings are stored securely and are accessible only to authorised personnel.
  - Personal Information: Staff/teachers must not share personal contact details (e.g., private phone numbers, social media accounts) with students/parents/guardians.
  - Background: Teachers delivering lessons from home must ensure backgrounds are professional, appropriate, and free of personal/sensitive information. Virtual backgrounds are encouraged.

- One-to-One Sessions: For one-to-one tutoring/consulting involving children, parents/guardians are encouraged to be aware of sessions and, where appropriate, present or nearby.

■ **Content and Conduct**

- Appropriate Content: All content accessed, created, or shared via company platforms or during company activities must be suitable for the educational environment and students' age.
- No Harmful Content: Creating, disseminating, or viewing offensive, illegal, discriminatory, or inappropriate material (e.g., pornography, hate speech, violent content) is strictly prohibited.
- Cyberbullying: Online bullying, harassment, or intimidation targeting students/staff is unacceptable and will result in disciplinary action.
- Impersonation: Users must not impersonate others online or create false profiles related to company activities.
- Copyright and Plagiarism: Respect intellectual property; plagiarism or copyright infringement is prohibited.

---

5. Communication: Email, Messaging, Social Media

1) **Staff and Teachers**

❖ Staff must not access social media, personal email, or other non-BBEVA websites during teaching hours/in front of students. Such access is limited to personal devices.

❖ When accessing social networks via personal devices, staff must exercise caution regarding posted content's potential impact on their professional position and BBEVA's reputation.

❖ BBEVA monitors all communications via its platforms and email addresses. Staff must immediately report any uncomfortable, insulting, discriminatory, threatening, or bullying communications to the DSL and IT team and must not respond. Staff must remain vigilant against fraudulent emails and report suspicious messages to IT.

❖ All online communications (using BBEVA or personal devices) must not intentionally or negligently:

- Endanger or cause harm to children/young people;

- Damage BBEVA's reputation;
- Breach confidentiality;
- Violate copyright;
- Breach data protection laws or engage in discrimination, bullying, or harassment, e.g.:
    - Making insulting/derogatory comments about gender reassignment, race (including nationality), disability, sexual orientation, religion/belief, or age;
    - Using social media to bully others;
    - Posting links to or endorsing discriminatory/offensive material.
      Under no circumstances may staff/teachers add students or parents/guardians as social media "friends" or contact students via social media.

2) **Students**

- Students should note that all communications via BBEVA platforms and email addresses are monitored.
  BBEVA's IT team works to ensure platform security. Spam and certain attachments are automatically blocked. If this hinders learning, students should contact IT support. Students must not respond to uncomfortable, insulting, discriminatory, threatening, or bullying communications and must report them immediately to the DSL/IT team or other staff.
- BBEVA expects students to carefully consider online posts (on personal or BBEVA social media) before sharing/endorsing content. Posts must not be inappropriate, offensive, or embarrassing to anyone (includes sexual, discriminatory, or offensive content).
- Students must report accidental access to violent/sexual content directly to the DSL/IT or staff. Deliberate access to inappropriate content will be recorded and handled per BBEVA's Behaviour and Discipline Policy.
- Storing/sharing/sending offensive/inappropriate messages/content via personal devices (even off-platform) violates the Behaviour and Discipline Policy. Issues will be escalated to the DSL, who may involve authorities/police.

---

6. Requirements for Camera Use

We recognise many students prefer interacting via camera/microphone, while others value text-only communication (due to special needs or to avoid distractions/anxiety). We aim to meet all students' needs by offering personalised learning experiences.
Our approach provides clear choices for communication tools, with parents/guardians informed if tools are used in class.
We expect all teachers to use cameras during online teaching and encourage students to do so. Benefits include:

- Stronger sense of community;
- Teachers can use visual cues to identify students needing help;
- Students can showcase work for immediate feedback.

To ensure safety, all camera users must follow our guidelines:

- Appropriate attire: Inappropriate clothing (e.g., pajamas, offensive slogans/images, vests, see-through garments) may result in removal from class.
- Background: Avoid distracting/filtered backgrounds; ensure no offensive posters/items are visible. Work in a quiet, plain environment.
- No third parties: Parents/siblings should not appear on camera during lessons.
- Privacy: Lesson recordings are accessible only to enrolled students, teachers, parents, and relevant BBEVA teams.
- Recording: All live lessons are recorded and stored securely for academic/safeguarding purposes.
- Device placement: Avoid private areas (e.g., bedrooms) for computers/laptops.
- Microphone use:
    - Students are encouraged to use microphones in group discussions.
    - Language must be professional (including from background family/friends).
    - Mute microphones when not speaking.
    - Avoid interrupting others; use the "raise hand" function and wait to be called on.

---

7. Reporting Procedures

Any E-Safety concerns, incidents, or suspected policy violations must be reported immediately:

1) Staff/Teachers: Report to the Designated Safeguarding Lead (DSL).

2) Students/Parents/Guardians: Report to a teacher/academic advisor (who will notify the DSL) or directly to the Designated Safeguarding Lead (DSL).
   Reports should include:

   - Date/time of incident.
   - Platform/device involved.
   - Description of the incident.
   - Individuals involved (if known).
   - Screenshots/evidence.

The DSL will assess and take appropriate action (e.g., internal investigation, disciplinary measures, parental liaison, or referral to external agencies like local authority children's services/police if child safeguarding concerns arise).

---

8. Filtering and Monitoring

1) For students learning from home, staff cannot fully prevent access to age-inappropriate websites. We rely on parent/guardian cooperation to monitor children's online activity. For students in BBEVA premises, we rely on the hosting BBEVA to implement appropriate filtering/monitoring.
2) Parents/guardians are strongly advised to filter/monitor children's online activity.
   If staff/students encounter inappropriate websites shared/posted on platforms, they should report them to the Senior Leadership Team.
3) BBEVA will report illegal online material (e.g., to IWF or CEOP).
4) Parents/guardians will be informed of any breaches of behaviour, safeguarding, anti-bullying, or E-Safety policies involving their child.

Effective classroom management and regular education on safe/responsible technology use are essential.

---

9. Data Storage and Processing

BBEVA fully complies with UK GDPR and the Data Protection Act 2018.

- All personal data (student records, communication logs, lesson recordings) is securely processed/stored.
- Data is collected only for lawful purposes, retained no longer than necessary, and

accessible only to authorised personnel.

- Individuals' data rights are respected.
- Our Privacy Policy (available on the company website) provides detailed information on data processing.

---

10. Password Security

Students and staff have individual work accounts. Password security is regularly emphasised. All students and staff must:

- Use strong passwords (≥8 characters, upper/lower case letters, numbers), changed every 3 months;
- Do not write down passwords;
- Do not share passwords with others;
- Use two-factor authentication (via app/SMS).

---

11. Safe Use of Digital and Video Images

1) Digital imaging offers significant learning benefits but carries risks (e.g., cyberbullying, stalking, grooming). Images may persist online indefinitely, causing harm/embarrassment.
2) Staff must educate students on risks related to capturing, using, sharing, posting, and distributing images—particularly self-posting on social media.
3) Parents/guardians/teachers/students must not casually record/create images of any part of BBEVA platforms (including lessons). To protect privacy/data, recordings/images must not be posted on blogs/social media.
4) Students must not capture, use, share, post, or distribute others' images unless for explicit educational purposes and/or authorised by staff.
5) Parents/guardians may capture digital images/videos of their child at BBEVA events for personal use (with staff permission) but must not post them without the consent of identifiable individuals.
6) Staff capturing digital images for educational purposes must follow this policy and the Acceptable Use of Technology Policy. Images must be taken on BBEVA devices only (not personal devices).
7) Written parental consent is obtained before publishing student photos on BBEVA's website (see Service Contract). Published photos are carefully vetted per good

practice guidelines.

8) Images must depict students appropriately and not engage in activities that risk personal/BBEVA reputation.

---

12. Misuse

1) BBEVA does not tolerate illegal/inappropriate activities in its environment and will report illegal activities to the police/authorities. If a child/young person is at risk due to online activity (e.g., cyberbullying, "sexting," extremism, grooming), BBEVA may seek external help.
2) Alleged misuse must be handled per BBEVA's policies/procedures (details in Safeguarding Policy).
3) BBEVA will sanction students misusing technology to bully/harass/abuse others (see Behaviour and Discipline Policy).

---

13. Electronic Devices - Search and Removal

BBEVA reserves the right to delete data from students' electronic devices. Staff discovering pornographic images (e.g., during screen-sharing) must report to the DSL/Head immediately for investigation.

Images found on phones/devices may be deleted unless required for police evidence. Staff must consider local regulations/guidelines and justify device searches/content removal.

---

14. Loading/Installing Software

Software loaded onto BBEVA systems or personal computers/devices must be legally licensed and virus-free.

Only authorised personnel (e.g., IT team) may load software onto platforms/BBEVA devices.

---

15. Backup and Disaster Recovery

BBEVA will define/implement backup strategies to restore critical systems/data within a reasonable timeframe after data loss.

---

16. Compliance, Sanctions, and Disciplinary Matters

Non-compliance exposes BBEVA to risks. Staff/teacher violations will be treated seriously and

may lead to disciplinary action (up to termination). Student violations are managed per the Behaviour and Discipline Policy (may include service suspension/cancellation). Serious violations (e.g., illegal activities/harm to children) will be reported to external agencies.

---

17. Policy Review and Updates

This E-Safety Policy will be reviewed annually by the Head and the Senior Leadership Team to ensure that it remains effective, up to date, and aligned with current legislation, statutory guidance, and best practice in online safety.

An earlier review may be undertaken if:

- New legislation, statutory guidance, or relevant regulatory requirements are introduced.
- Significant developments in technology or online risks arise that impact the safeguarding of students and staff.
- A serious e-safety incident occurs, which highlights the need for changes to existing procedures.

Any significant updates to this policy will be shared with staff, students, and parents/carers as appropriate.

For E-Safety questions/concerns about this policy, contact our Designated Safeguarding Lead (DSL):

Mr. Chris Davies

Email: chris.jdavies@live.co.uk

Tel: +44 7796756817

Last Reviewed: August 2025

Next Review: August 2026

Policy Owner: Designated Safeguarding Lead (DSL)