



Emil Dale Academy – Online Safety Policy

Contents

1. Purpose 3

2. Scope 3

3. Policy Principles..... 3

4. Online Conduct and Behaviour 3

5. Online Teaching and Learning Environments 4

6. Safeguarding and Reporting..... 4

7. Digital Security and Data Protection 4

8. Use of Social Media 4

9. Breaches and Disciplinary Action 5

10. Training and Awareness 5

11. Linked Policies 5

12. Contacts 5

13. Document Control..... 6

1. Purpose

1. The purpose of this policy is to ensure that all members of Emil Dale Academy (EDA) use online technologies in a safe, responsible, and respectful manner. It aims to:
 - a. Safeguard students from online harm, abuse, or exploitation.
 - b. Promote positive digital citizenship and professional conduct online.
 - c. Ensure compliance with legal and regulatory frameworks including the UK Data Protection Act 2018, GDPR, Prevent Duty, Keeping Children Safe in Education (KCSIE), and the university/college partners' safeguarding expectations.
 - d. Protect the reputation of Emil Dale Academy and its community.

2. Scope

2. This policy applies to all students and staff involved in the delivery, support, or assessment of EDA's educational programmes, including:
 - a. The Sixth Form (BTEC Level 3), validated by North Hertfordshire College (Year 12) and The Knights Templar School, Baldock (Year 13).
 - b. The CertHE and BA (Hons) in Musical Theatre, validated by the University of Bedfordshire.
3. It covers all online activity conducted through academy systems and platforms, including but not limited to:
 - a. EDA emails and learning platforms (e.g., Google Workspace, Moodle, Microsoft Teams).
 - b. Social media use related to EDA.
 - c. Online auditions, assessments, and classes conducted via video conferencing.
 - d. Any device used on the EDA network or for EDA-related communication.

3. Policy Principles

4. EDA promotes an environment where digital activity reflects the values of Respect, Integrity, Professionalism, and Safety. All users must:
 - a. Treat others with respect online.
 - b. Protect their personal information and that of others.
 - c. Use academy technology responsibly and only for legitimate educational or professional purposes.
 - d. Report any concerns or breaches promptly.

4. Online Conduct and Behaviour

5. Students are expected to:
 - a. Communicate professionally in all online interactions with peers, staff, and industry professionals.
 - b. Avoid any language, images, or behaviour that could be considered offensive, discriminatory, or harassing.
 - c. Use their EDA email for academy business only.
 - d. Not share meeting links, recordings, or passwords without permission.
 - e. Obtain consent before sharing or uploading any image, video, or performance footage featuring others.
 - f. Respect copyright and intellectual property rights.

- g. Ensure that online profiles (e.g. social media, professional portfolios) represent themselves and EDA positively.

5. Online Teaching and Learning Environments

6. EDA staff and students will:
 - a. Use approved platforms only for virtual learning.
 - b. Ensure that video conferencing sessions are secure (password protected, waiting rooms enabled, no unauthorised recording).
 - c. Dress appropriately and behave as they would in a physical classroom.
 - d. Choose appropriate backgrounds and environments for online participation.
 - e. Avoid using mobile devices during online learning unless required for the activity.

6. Safeguarding and Reporting

7. EDA takes online safety as part of its broader Safeguarding and Prevent duties.
8. Any online safeguarding concern, including cyberbullying, grooming, or exposure to harmful content, must be reported immediately to the Designated Safeguarding Lead (DSL) or a Deputy DSL.
9. For under-18 students, the same reporting procedures apply as in the Safeguarding and Child Protection Policy.
10. For HE students, concerns should be reported to the HE Safeguarding Officer or Head of Student Services, who will liaise with the University of Bedfordshire's safeguarding team if appropriate.

7. Digital Security and Data Protection

11. All users must follow the EDA Data Protection Policy.
12. Devices should be secured with passwords and kept updated.
13. Personal data (including student records, performance footage, or contact lists) must not be stored on personal devices unless authorised and encrypted.
14. Online files and recordings must be stored in EDA-approved cloud storage only.
15. Breaches of data security must be reported immediately to the Data Protection Officer (DPO).

8. Use of Social Media

16. This policy must be read in conjunction with the Social Media Policy.
17. EDA recognises the professional importance of social media for performing arts students but expects responsible use.
18. Students and staff must not:
 - a. Post or share content that could bring EDA or its partners into disrepute.
 - b. Share confidential or identifiable information about students or staff.
 - c. Engage in online arguments, harassment, or defamation.
 - d. Impersonate EDA accounts or misrepresent affiliation.

19. EDA may issue guidance or intervene in cases where social media activity poses reputational, safeguarding, or wellbeing risks.

9. Breaches and Disciplinary Action

20. Breaches of this policy may result in disciplinary action under:
- a. The Student Code of Conduct (for students).
 - b. The Staff Disciplinary Policy (for staff).
 - c. Serious incidents may also be referred to law enforcement or regulatory authorities.

10. Training and Awareness

21. Online safety is embedded in induction and ongoing pastoral programmes.
22. Staff receive regular training as part of safeguarding and GDPR development.
23. The policy will be reviewed annually to reflect evolving technology and best practice.

11. Linked Policies

24. This policy should be read in conjunction with:
- a. Safeguarding and Child Protection Policy
 - b. Prevent Policy
 - c. Data Protection and GDPR Policy
 - d. Acceptable Use Policy (IT)
 - e. Student Code of Conduct
 - f. Social Media Policy
 - g. Complaints and Whistleblowing Policies

12. Contacts

25. Designated Safeguarding Lead (DSL): Victoria Hammond vicky@emildale.co.uk

26. Deputy DSLs:

Sarah Moore sarah@emildale.co.uk

Siobhan Kelly siobhan@emildale.co.uk

Jonathan Hunt jonathan@emildale.co.uk

Other Safeguarding Officers:

Marina Abdeen marina@emildale.co.uk

Rachel Saunders rachel@emildale.co.uk

Melissa Joseph melissa@emildale.co.uk

27. Data Protection Officer (DPO): Sarah Moore sarah@emildale.co.uk

13. Document Control

Version Number	Date of Issue	Review Date	Author	Changes Made/ detail
01	20.10.2025	September 2026	Sarah Moore	First draft