National Extension College

Online Safety Policy

VERSION : 1.0
LAST REVISED : FEBRUARY 2025
NEXT REVIEW DATE :

Online Safety Policy

Regulatory Compliance

- Online Safety Act 2023
- Keeping Children Safe in Education (KCSIE) September 2024
- Ofcom Online Safety Regulations
- UK GDPR (Data Protection Act 2018)
- Prevent Duty (Counter-Terrorism and Security Act 2015)
- Cyber Security and Resilience Bill (anticipated legislation)

1. PURPOSE AND PRINCIPLES

NEC is committed to ensuring a **safe, respectful, and legally compliant** online learning environment for all students, staff, and tutors. This policy sets out **clear expectations, monitoring, and response mechanisms** to protect students, particularly **minors and vulnerable learners**.

NEC upholds the following core principles:

- **Safeguarding all users**, particularly those under 18 or in vulnerable groups.
- **Ensuring legal compliance** with UK online safety laws and educational regulations.
- **Preventing exposure** to harmful, illegal, inappropriate, or extremist content.
- **Promoting responsible online behaviour** and respectful interactions.
- **Protecting personal data and ensuring digital security** to mitigate cyber threats.

2. SCOPE

This policy applies to:

- All NEC students, including **minors and adult learners.**
- NEC **staff, tutors, and moderators.**
- NEC's **third-party IT providers and external partners.**

It covers:

- **NEC online learning platforms** (VLE, forums, discussion boards).
- **NEC communication channels** (email, messaging, video conferencing).
- **NEC-controlled social media accounts**.
- **Cybersecurity protections** for students, staff, and NEC's infrastructure.

3. ROLES AND RESPONSIBILITIES

3.1 NEC's Online Safety Governance

- **Designated Online Safety Lead (DOSL):** Ensures compliance, oversees safety incidents, and escalates major concerns.
- **Deputy Online Safety Lead (DOSL):** Supports and deputises for the DOSL.
- **Designated Safeguarding Lead (DSL):** Oversees child protection and online safeguarding referrals under **KCSIE 2024**.
- **IT & Technical Support Team:** Implements cybersecurity measures and ensures compliance with **UK GDPR.**
- **Moderators & Tutors:** Monitor student interactions and escalate concerns when necessary.

3.2 Responsibilities of Users

- **Staff & Tutors:**
    - Follow NEC's **ICT Security Policy** and **Acceptable Use Policy (AUP).**
    - Report **any safeguarding or online safety concerns** immediately.
    - Maintain professional boundaries in all online interactions.
- **Students:**
    - Adhere to the **Student Acceptable Use Agreement (AUA)**.
    - Report any **inappropriate or concerning behaviour** via NEC's reporting system.
    - Use NEC forums and platforms **responsibly and respectfully.**
- **Parents/Guardians (for under-18 students):**
    - Reinforce NEC's online safety guidelines at home.
    - Monitor online activity where appropriate and report concerns to NEC.

4. ACCEPTABLE USE OF DIGITAL PLATFORMS

4.1 Staff & Tutor Responsibilities

- Use NEC digital platforms **for educational purposes only.**
- **No private communication** with students outside NEC's monitored systems.
- **Do not share** personal contact details or social media accounts with students.
- **Ensure that all teaching materials** comply with copyright laws and safeguarding requirements.

4.2 Student Responsibilities

- **No sharing of personal details** (addresses, phone numbers, social media).
- **No cyberbullying, harassment, or inappropriate language.**

- **No posting or accessing illegal, extremist, or harmful content.**
- **No private messaging between minors and adult learners** in NEC forums.

4.3 Online Forum Rules

- Respectful and academic discussions only.
- No unmoderated private messaging.
- No inappropriate, offensive, or extremist content.

5. MONITORING, MODERATION, AND REPORTING

5.1 Moderation Approach

NEC employs a **blended moderation** system that includes:

- **Human moderation** for flagged discussions and sensitive topics.
- **Regular audits** of forum discussions and online interactions.

5.2 Reporting Online Safety Concerns

Users can report concerns through: **Direct escalation student.support@nec.ac.uk**

All reported concerns will be reviewed and triaged, with high risk cases escalated as a matter of urgency.

5.3 Escalation Pathways for Serious Concerns

Incident Type	Escalation Path
Cyberbullying or Harassment	NEC Moderation Team → DOSL → DSL if under 18
Online Grooming or Exploitation	NEC Safeguarding Team → CEOP / Police
Radicalisation or Extremism	DSL → Prevent Duty Officer
Data Breaches or Hacking Attempts	IT Security → Data Protection Officer

6. CYBERSECURITY AND DATA PROTECTION

6.1 Cybersecurity Measures

- **Multi-factor authentication (MFA)** for NEC platforms.
- **Data encryption** to protect student information.

- **Strict access controls** for staff and tutors.
- **Regular security audits** to prevent cyber threats.

6.2 Data Protection Compliance

NEC adheres to:

- **UK GDPR (Data Protection Act 2018)** for personal data handling.
- **Ofcom's Online Safety Regulations** to prevent harmful content exposure.
- **KCSIE 2024 guidelines** for protecting minors online.

7. CONSEQUENCES FOR POLICY VIOLATIONS

Violation	Consequence
Minor misconduct (e.g., inappropriate language)	Formal warning, content removal
Repeated misconduct	Forum restrictions, temporary ban
Serious breach (e.g., grooming, radicalisation)	Permanent ban, report to authorities

All safeguarding concerns involving under-18s are escalated to the DSL and external agencies as required.

8. COMPLIANCE AND POLICY REVIEW

- NEC ensures **compliance with the Online Safety Act 2023** and **KCSIE 2024**.
- **Annual policy review** conducted to reflect legal and regulatory updates.
- **Trustees oversee** policy effectiveness and implementation.

9. ONLINE SAFETY RISKS: THE 4Cs FRAMEWORK

To ensure a **safe and secure** online learning environment, NEC addresses the **four key areas of online safety risk: Content, Contact, Conduct, and Commerce.**

9.1 Content Risks

Students may encounter harmful or misleading content online. NEC takes proactive measures to **moderate, and educate** users on risks such as:

- **Violent or extremist material** that promotes hate speech or radicalisation.
- **Pornographic or sexually explicit content,** which is inappropriate for students.
- **Misinformation and fake news,** which can distort knowledge and critical thinking.
- **Content promoting self-harm, suicide, or eating disorders,** which poses a serious mental health risk.

To mitigate these risks:

- Students are encouraged to **report inappropriate material** through NEC's reporting system.
- Tutors and moderators receive **guidance on handling sensitive discussions** responsibly.

9.2 Contact Risks

Online interaction comes with potential dangers, particularly in an educational setting. NEC safeguards students from:

- **Online grooming and exploitation by predators.**
- **Cyberbullying and harassment in forums or communication channels.**
- **Unwanted or inappropriate contact from strangers.**
- **Phishing scams designed to steal personal or financial information.**

To prevent these threats:

- All **student-tutor communication** is conducted within **NEC-monitored platforms** (no private messaging outside official systems).
- NEC **prohibits private communication between minors and adult learners** in forums.
- Tutors and moderators are trained to **identify and escalate concerns** regarding grooming or online abuse.

9.3 Conduct Risks

Students' own behaviour online can also pose risks to their safety and reputation. NEC promotes **responsible digital citizenship** by highlighting:

- The importance of **not sharing personal details** (e.g., phone numbers, addresses, social media).
- The dangers of **engaging in cyberbullying, hate speech, or harmful interactions.**
- The long-term impact of **posting inappropriate content** (e.g., offensive remarks, misleading information).
- The risks of **falling for online scams or engaging in illegal activities.**

To reinforce safe conduct:

- All students agree to a **Student Acceptable Use Agreement (AUA)** as part of the Terms and Conditions of enrolment outlining responsible behaviour.
- Tutors model **positive online interactions** and reinforce professional conduct.
- NEC has **clear consequences** for violations, ranging from formal warnings to removal from courses.

9.4 Commerce Risks

Financial risks are often overlooked in education but are increasingly relevant in online spaces. NEC recognises threats such as:

- **Fraudulent websites or fake NEC-branded scams** attempting to steal student information or payments.
- **In-app purchases and excessive spending** in educational tools or external platforms.
- **Identity theft and financial data breaches**, particularly with online payments.
- **Gambling and exploitative monetisation strategies** embedded in some digital platforms.

To protect students:

- NEC signposts students to **guidance on safe online payments** and **how to recognise fraudulent schemes.**
- Data protection measures, including **encryption and multi-factor authentication (MFA),** secure student accounts.
- Students are warned **never to share financial details** with anyone claiming to represent NEC outside official communication channels.

10. COMMITMENT TO ONLINE SAFETY

NEC is committed to educating, protecting, and empowering all students in navigating digital spaces safely. We continuously review and update our policies to align with **best practices in online safety, safeguarding, and cybersecurity.**

For any concerns or further guidance, students, tutors, and parents are encouraged to reach out to NEC's **Designated Online Safety Lead (DOSL), Safeguarding Team, or IT Security Team** via email students.support@nec.ac.uk.

Revision History

Version	Last revised	Next review date	Policy Owner	Notes
Version 1.0	Feb 2025	Feb 2026	DSL and Deputy DSL	