

Digital Conduct and Communications Policy

05 May 2026, 8 min read

Operated by: Nudge Education Ltd · **Version:** Dec 2025 · **Owner:** Director of Operations

Digital Conduct and Communications Policy December 2025 Review date: December 2025

This policy applies to all individuals working with or on behalf of Nudge Education, including permanent staff, sessional practitioners, contractors, volunteers, and any third-party professionals who access our systems, work with students, or handle sensitive information. Everyone in these roles has a responsibility to uphold safe, respectful, and secure digital practices in line with safeguarding, data protection, and professional standards.

Digital Conduct and Communications Policy December 2025
Introduction and Purpose

At Nudge Education, technology plays a vital role in how we support the children and young people we serve. Whether it's remote learning, online communication, or day-to-day administration, we are committed to ensuring that all digital tools are used responsibly, securely and in a way that upholds the trust placed in us.

This policy outlines our expectations for the use of IT systems, mobile devices and social media in professional contexts. It is grounded in the principles of safeguarding, data protection, and respectful conduct and applies to all staff, contractors, volunteers, and third-party professionals who work under the umbrella of Nudge Education.

We are not a school, but we have the same moral and legal responsibilities to protect the wellbeing, privacy and dignity of the young people and families we serve. That includes what we allow them to access online and how we communicate with them.

Use of IT and Online Access

Staff may use IT equipment in a variety of settings including public libraries or community centres during educational delivery. When doing so, it is important to ensure that security controls are in place to restrict access to inappropriate or harmful content.

When working in public or shared spaces, staff must take care to prevent sensitive data from being seen or shared unintentionally. This includes protecting screens, using secure Wi-Fi connections, and ensuring that any digital records, especially those involving students or commissioners are stored and transmitted securely.

All data should be accessed and shared via secure platforms. Currently, Nudge Education uses Google Drive to store documentation related to company operations, commissioned work and student records. If a commissioner requests an alternative data-sharing method, we will explore secure alternatives that align with our resources.

Digital Conduct and Communications Policy December 2025

Mobile Devices and Mobile Telecommunications

Staff may be provided with mobile devices by Nudge Education, but more commonly, contractors are expected to use their own equipment. Regardless of whether the device is personal or provided by the organisation, all must meet minimum security requirements.

Devices must be protected by a strong password or biometric lock and, where possible, must use two-factor authentication when accessing sensitive information. Devices should never be left unattended in public spaces, and any loss, theft or suspected breach must be reported immediately to the Data Protection Officer.

Staff must not use personal mobile phones to contact students or families, either via call, text or messaging apps. All communications with students and families must go through official Nudge Education channels such as your Nudge email address or an authorised platform and should be logged or auditable. Similarly, students or families must not be permitted to use your personal mobile device under any circumstances, even in emergency situations.

If students require access to a phone during provision (for example, to contact a parent in an emergency), this must be facilitated under supervision, using agreed safeguarding procedures.

If you receive a personal message or phone call from a student after the intervention period has ended, you are required to report this to your Education Case Manager. Any concerns regarding inappropriate contact by any means must be escalated without delay.

If it is found that this policy has not been followed, disciplinary action may be taken that could result in dismissal and reporting to the Local Authority Designated Officer (LADO) for that region.

Filtering and Monitoring

Although Nudge Education is not a school, we share the same commitment to keeping young people safe in their use of technology. We recognise the risks posed by access to harmful, inappropriate, or illegal content online, whether during education sessions or in the student's own time.

Digital Conduct and Communications Policy December 2025

Staff delivering online or in-person provision should take steps to ensure that students are not exposed to harmful or inappropriate content during sessions. This may involve checking shared screens, supervising device use during tasks, and monitoring browser tabs where feasible.

Where students are using their own devices during sessions, staff should remain alert to signs that they may be accessing inappropriate content and respond in line with safeguarding guidance. If you become aware that a student is accessing harmful material outside of sessions, or if they disclose concerning online activity, this must be reported as a safeguarding concern.

We expect all staff to foster open, age-appropriate conversations with students about staying safe online, and to direct them to positive, safe digital resources. While we cannot monitor students' personal internet use outside of sessions, we have a duty to act when risks are known or suspected.

Social Media and Public Platforms

Nudge Education encourages all team members to present themselves professionally online, just as they would in the workplace. This applies across

all social media platforms, including Facebook, Instagram, X (formerly Twitter), TikTok, YouTube, personal blogs, forums, and other online communities.

Employees and contractors must not share any confidential, sensitive, or identifying information about students, families, commissioners, or the organisation. Posts must not compromise professional boundaries, bring Nudge Education into disrepute, or cause harm to others.

Connecting with students via personal social media accounts is strictly prohibited. All online engagement with students must be conducted through official Nudge Education accounts or approved platforms and only during the period of active engagement. Failure to comply with this policy could lead to disciplinary action that could result in dismissal and reporting to the Local Authority Designated Officer (LADO) for that region.

If you come across concerning content online related to Nudge Education or to any of the young people you are supporting, this should be reported to the Senior Management Team or Designated Safeguarding Lead.

Digital Conduct and Communications Policy December 2025 Online Tuition and Virtual Sessions

All online tuition must be conducted using the platforms authorised by Nudge Education. These platforms have been selected to ensure that sessions are safe, secure, and quality assured.

Practitioners must be dressed appropriately, based in a private setting, and ensure there are no distractions during sessions. No recordings or screenshots are permitted unless explicitly authorised by Nudge Education for safeguarding or quality assurance purposes.

During online sessions, practitioners must be vigilant for any signs of distress, abuse, or inappropriate behaviour. Safeguarding concerns must be acted on immediately, using the reporting process outlined in the organisation's Safeguarding Policy.

When sharing screens, care must be taken to ensure that no personal or inappropriate content (e.g. tabs, images, notifications) is visible to the student. Shared resources must be suitable for the learner's age, needs, and background.

Artificial Intelligence (AI) Tools

We recognise the potential of AI tools to support our work, but also acknowledge the risks involved. AI should never be used to process personal data such as student records, commissioner details, or identifiable content without the explicit approval of the Data Protection Officer.

Where AI tools are approved for use, the results must be carefully checked for accuracy, relevance, and bias. The human professional remains fully responsible for the content generated and how it is used in practice.

Any proposed use of AI tools that involves personal data will require a Data Protection Impact Assessment (DPIA) and must be justified, documented, and risk-assessed in accordance with our AI Policy.

Digital Conduct and Communications Policy December 2025 Cybersecurity and Data Protection

All staff are required to complete regular training in data protection and cybersecurity. Devices and platforms used in the course of your work must be kept secure, up to date, and password protected.

You must only access data that is necessary for your role and must store and share that data using approved methods. All data handling must comply with the principles of the UK General Data Protection Regulation (UK GDPR), including fairness, transparency, data minimisation, and security.

Any data breaches, unauthorised disclosures, or cyber incidents must be reported immediately to the Data Protection Officer.

Compliance and Monitoring

This policy is overseen by the Data Protection Officer and the Senior Management Team. Non-compliance with any part of this policy may lead to disciplinary action, termination of contract, and in some cases, reporting to external commissioners or regulators.

Review and Ownership

This policy is reviewed annually or as required, in response to legislative updates, emerging risks, or changes in organisational practice.

Change History Record

Version Date Details of Change(s) Approved By 2.0 5/12/2025 Implementation of V2 policy Brian Mair

Digital Conduct and Communications Policy December 2025

Document control

Field	Value
Version	Dec 2025
Owner	Director of Operations
Status	live
Source file	1. All Company/Digital Conduct and Communications Policy - Dec 2025.pdf