



EDClass Staff Code of Conduct and acceptable use Policy

POL083

Issue number 1

Approved by Sam Warnes

EDClass Staff Code of Conduct and Acceptable Use Policy

Introduction

EDClass provides an accredited online alternative education provision delivering personalised distance learning and live academic interventions for pupils across the UK. Many learners accessing EDClass have complex profiles, including Special Educational Needs and Disabilities (SEND), Education, Health and Care Plans (EHCPs), medical conditions, social, emotional, and mental health (SEMH) difficulties, or are accessing education via internal alternative provision (IAP), isolation, or part-time timetabled seat allocations.

Operating exclusively within a remote digital environment requires the highest standards of professional conduct, digital ethics, and safeguarding discipline. The physical distance between practitioners and pupils does not diminish professional boundaries; rather, it demands absolute transparency, structured communication, and rigorous adherence to auditable systems.

Scope

This policy applies to all individuals working on behalf of EDClass, including:

- ✓ Directly employed UK-qualified teachers, subject specialists, and academic tutors.
- ✓ Safeguarding and pastoral welfare personnel.
- ✓ School account managers, administrative coordinators, and technical support staff.
- ✓ Agency workers, self-employed contractors, and software developers accessing production environments.

Compliance with this Code of Conduct is a mandatory contractual condition of employment. Failure to uphold these standards may result in disciplinary action up to and including summary dismissal for gross misconduct, referral to the Teaching Regulation Agency (TRA), and referral to the Disclosure and Barring Service (DBS).

Core Professional Standards and Relational Ethos

All staff members act as ambassadors for EDClass and role models for learners. Staff must uphold the **DfE Teachers' Standards** (Part Two: Personal and Professional Conduct) and demonstrate:

- ✓ **Uncompromising Safeguarding Vigilance:** Prioritising the welfare, psychological safety, and physical protection of every learner in every interaction.
- ✓ **Trauma-Informed Practice:** Approaching learners with empathy, consistency, and positive unconditional regard, recognising that placements represent targeted interventions to break barriers to learning rather than punitive destinations.
- ✓ **High Expectations and Inclusive Delivery:** Setting aspirational academic and personal goals, scaffolding tasks to accommodate neurodiversity and learning differences, and maintaining belief in every pupil's capacity to achieve.

- ✓ **Equality, Diversity, and Respect:** Complying with the Equality Act 2010 by actively challenging discrimination, promoting mutual respect, and honouring protected characteristics across all digital communications.
- ✓ **Restorative Behaviour Management:** Applying EDClass's behaviour repair strategies calmly and objectively, rejecting punitive, sarcastic, or confrontational methods during moments of pupil dysregulation.

Online Professional Boundaries and Communication Protocols

The digital nature of EDClass requires strict boundaries to eliminate ambiguity and serve a **dual-protection purpose**: safeguarding vulnerable learners from a vast range of situations, while simultaneously shielding teachers from unfounded allegations by eliminating unmonitored, private interactions.

- ✓ **Exclusive Platform Use:** Confines all educational and pastoral communication strictly to the monitored EDClass portal. Bypassing the system to use external communication tools is prohibited, ensuring every exchange remains within institutional oversight.
- ✓ **Zero Direct Contact:** Imposes an absolute ban on personal contact channels. Staff must never share or interact via personal phone numbers, private email addresses, personal social media profiles, or gaming networks.
- ✓ **Auditable Sessions:** Ensures every interaction—including video feeds, chat logs, whiteboard drawings, and system timestamps—is recorded and archived. This creates an immutable, tamper-evident audit trail that provides definitive factual evidence if an allegation or welfare incident arises.
- ✓ **Professional Scrutiny:** Sets a transparent professional standard. Staff must conduct all interactions with the understanding that every message, tone, and visual stream can be scrutinised at any time by commissioning school leaders, parents, and regulatory inspectors.

Approved Communication Channels

- ✓ **Platform Exclusivity:** All instructional delivery, academic feedback, and pastoral check-ins must occur exclusively through the designated EDClass virtual classroom, secure chat engine, or authorised administrative dashboards.
- ✓ **Prohibited Channels:** Staff must never communicate with enrolled learners, former learners under 18, or vulnerable young people using:
 - Personal or corporate email addresses outside platform chat workflows.
 - Personal mobile devices, landlines, or SMS text messaging.
 - External messaging platforms (e.g., WhatsApp, Telegram, Signal, Discord).
 - Video conferencing software outside the platform (e.g., personal Zoom, Teams, Google Meet).
 - Online gaming networks, consoles, or interactive digital spaces.

Social Media and Online Presence

- ✓ Staff must not initiate, accept, or tolerate social media contact with current or former EDClass learners on any public or private network (including Instagram, TikTok, Snapchat, Facebook, X, LinkedIn, or Twitch).
- ✓ Staff must maintain strict privacy settings on all personal social media profiles and ensure that personal profiles do not mention specific learners, commissioning schools, or operational incidents.
- ✓ Staff must not post images, materials, or opinions online that bring EDClass into disrepute, undermine their professional standing as educators, or compromise child protection standards.
- ✓ If a learner attempts to follow or contact a staff member on an external platform, the employee must reject/ignore the request immediately, take a screenshot, and log the occurrence as an alert to **Kim, Head of Safeguarding**.

Gifts, Favouritism, and Personal Relationships

- ✓ Staff must treat all learners equitably. Showing favouritism, establishing exclusive relationships, or developing "special" confidences with individual learners is strictly prohibited.
- ✓ Staff must not purchase, send, or promise physical gifts, electronic vouchers, gaming currency, or financial rewards to learners.
- ✓ Any pastoral encouragement must occur through approved platform reward tools and formal learner praise mechanisms.

Virtual Classroom Protocols and Video/Audio Standards

In line with the DfE Online Education Accreditation Scheme (OEAS Standard 4), live instructional delivery must maintain structured pedagogical and physical safeguards:

Environment and Staging

- ✓ **Physical Workstation:** Staff delivering live teaching or video support must work from a private, secure location where domestic routines, third parties, or unvetted individuals cannot overhear pupil conversations or view platform screens.
- ✓ **Visual Background:** Teachers must deliver instruction against an approved, neutral corporate background or active platform blur filter. No personal family photographs, political slogans, inappropriate artwork, or domestic items should be visible.
- ✓ **Audio Privacy:** Headsets with integrated noise-cancelling microphones must be used for all live voice/video calls to prevent household audio from entering the session and ensure learner audio remains confidential.

Dress Code and Personal Presentation

- ✓ Staff appearing on camera must maintain professional business-casual dress appropriate for an on-site educational institution.
- ✓ Revealing, casual loungewear, gym attire, or clothing displaying political slogans, commercial logos, or controversial imagery is prohibited.

Live Session Management

- ✓ **Dual Monitoring and Transparency:** Staff must always operate under the knowledge that every keystroke, lesson delivery session, whiteboard illustration, and audio/video feed is logged, recorded, and subject to quality assurance and safeguarding audits.
- ✓ **Learner Webcams:** When a learner turns on their camera, staff must verify that the pupil is in an appropriate environment (e.g., seated at a desk or living space, fully dressed). If a pupil connects from a private bed or an inappropriate domestic setting, the teacher must calmly ask them to relocate or disable the camera, logging the event immediately for pastoral review.
- ✓ **Refusal to Record Off-System:** Staff are prohibited from making local, unapproved screen recordings, screenshots, or audio captures of learners on personal storage devices or unauthorised local hard drives.

Acceptable Use of Technology, Hardware, and Infrastructure

To maintain organisational cybersecurity, prevent operational downtime, and ensure data integrity, all personnel must follow strict technical use guidelines:

Device Security and Access Management

- ✓ **Authorised Devices Only:** Platform access for teaching and administration must take place on EDClass-managed equipment or strictly vetted devices compliant with enterprise Mobile Device Management (MDM) security controls.
- ✓ **Credential Protection:** Staff are assigned unique, individual credentials. Sharing accounts, passwords, or Multi-Factor Authentication (MFA) tokens is a severe disciplinary infraction.
- ✓ **Password Standards:** Passwords must meet modern enterprise complexity standards (minimum 14 characters, combining cases, numbers, and symbols) and be rotated per IT protocols.
- ✓ **Auto-Lock Policy:** Staff must lock their workstations whenever leaving their desk, ensuring sessions auto-lock after a maximum of 5 minutes of inactivity.

Clean-Screen and Screen-Sharing Protocols

When utilising screen-share or live-casting tools during lessons:

- ✓ Staff must close all unrelated browser tabs, private email clients, administrative spreadsheets, and internal messaging channels before initiating a screen-share.
- ✓ Staff must never share a full desktop display containing student profile lists, SENCo emails, or safeguarding dashboards.
- ✓ Personal browsing during live shifts is strictly prohibited on production workstations.

Prohibited System Activities

Staff must not:

- ✓ Attempt to bypass, reconfigure, or disable EDClass filtering, monitoring, antivirus, or firewall appliances.
- ✓ Use Virtual Private Networks (VPNs) or proxy tunnels to mask network traffic unless authorised by the Technical Director.
- ✓ Download, store, or execute unauthorised commercial software, games, peer-to-peer torrents, or malicious code on work devices.
- ✓ Connect unapproved, non-encrypted external USB drives or portable media storage devices to company hardware.
- ✓ Input confidential learner personal data or operational records into unapproved third-party commercial artificial intelligence engines.

Information Security, Data Protection, and Learner Confidentiality

This framework operationalises the Data Protection Act 2018 and UK GDPR across EDClass, specifically governing how staff handle special-category data—such as medical indicators, child protection histories, and statutory Section F provisions (the legally binding special educational support outlined in an Education, Health and Care Plan).

Legal Context: Data Processor vs. Data Controller

Under UK data protection law, the commissioning school or local authority acts as the Data Controller (holding legal ownership of the pupil's official educational record), while EDClass acts as the Data Processor (delivering alternative provision on their behalf).

Because EDClass handles high-risk, special-category data belonging to vulnerable pupils, staff are bound by strict protocols governing access, data sharing, and security boundaries.

Decision Matrix Breakdown

- ✓ **Confidential Safeguarding Disclosures:**
 - ✓ **Rule:** Never promise secrecy or unconditional confidentiality to a pupil.
 - ✓ **Action:** Record the student's exact words verbatim within the internal safeguarding repository (EDSafe).
 - ✓ **Rationale:** In UK law and statutory safeguarding guidance (KCSIE), child safety strictly overrides personal privacy. Verbatim recording ensures an objective, unvarnished legal record that is not compromised by staff interpretation.
- ✓ **Parental Requests for Operational or Assessment Reports:**
 - ✓ **Rule:** Never release progress, attendance, or assessment reports directly to parents.
 - ✓ **Action:** Direct parents to the commissioning home school's Main Point of Contact (MPOC) or Special Educational Needs Coordinator (SENDCo).
 - ✓ **Rationale:** Because the commissioning school is the legal Data Controller, all formal records, Subject Access Requests (SARs), and statutory updates must

be vetted and released through the home school to avoid disclosing restricted third-party data or conflicting with local multi-agency plans.

- ✓ **Reviewing Learner Profiles (Data Containment):**
 - ✓ **Rule:** Restrict all viewing strictly to the live platform interface.
 - ✓ **Action:** Never export, download, screenshot, or print records to personal hard drives, external USBs, personal cloud storage, or paper files.
 - ✓ **Rationale:** Prevents data exfiltration and loss of custody. Special-category data must remain within the secure, encrypted, and access-logged platform environment to prevent accidental disclosure or physical loss.
- ✓ **Unauthorised Data Breaches or Misdirection:**
 - ✓ **Rule:** Immediate internal reporting within **under 1 operational hour**.
 - ✓ **Action:** Notify the organisation's Data Protection Lead (DPO) and the Head of Safeguarding (Kim) instantly upon identifying any misdirected email, compromised login, or data exposure.
 - ✓ **Rationale:** The Information Commissioner's Office (ICO) mandates that significant data breaches must be formally notified within **72 hours** of becoming aware of them. A strict 1-hour internal reporting threshold ensures the incident response team has maximum time to contain the leak, assess the harm to vulnerable minors, and notify the commissioning school and regulator if required.

Confidentiality vs. Safeguarding

- ✓ **No Promise of Secrecy:** Staff must never promise confidentiality to a learner. If a child begins to disclose information regarding abuse, neglect, exploitation, or criminal activity, staff must clearly and gently explain that they have a duty to pass the information to **Kim, Head of Safeguarding**, to ensure the learner remains safe.
- ✓ **Need-to-Know Principle:** Information regarding SEND diagnoses, medical alerts, or child protection markers must be accessed only when required to adapt lessons and support the learner's well-being. Staff must not discuss learner details with colleagues who are not involved in their educational provision.
- ✓ **Physical Data Security:** Staff must not print paper copies of learner profiles, EHCPs, safeguarding case files, or attendance records outside of authorised office locations. Any physical documentation must be shredded using cross-cut shredders immediately after use.

Managing Low-Level Concerns and Allegations Against Staff

In compliance with **KCSIE 2026 (Part Four)** and **OEAS Standard 5**, EDClass maintains a culture of openness and accountability regarding adult conduct.

Low-Level Concerns Framework

A "low-level concern" is any concern—no matter how small, and even if no more than a nagging doubt—that an adult working in or on behalf of EDClass may have acted in a manner inconsistent with this Code of Conduct, but which does not meet the legal threshold for significant harm.

Examples include:

- ✓ Using overly familiar, informal, or affectionate language with a learner in platform chat.
- ✓ Remaining logged into a 1:1 call with a learner without clear instructional purpose.
- ✓ Displaying momentary frustration, sarcasm, or inappropriate humour during live instruction.
- ✓ Inadvertently sharing an unapproved personal detail or social media handle.

Reporting Procedure:

- ✓ All low-level concerns regarding colleagues or oneself (self-reporting is encouraged to maintain transparency) must be submitted in writing to **Kim, Head of Safeguarding**, within **24 hours**.
- ✓ The Head of Safeguarding will investigate the context, record the concern confidentially, evaluate whether a pattern exists, and determine whether informal remediation, coaching, or formal review is necessary.

Formal Allegations That Meet the Harm Threshold

Where an allegation suggests that a member of staff has:

- ✓ Behaved in a way that has harmed a child, or may have harmed a child;
- ✓ Possibly committed a criminal offense against or related to a child;
- ✓ Behaved towards a child in a way that indicates they may pose a risk of harm if they work regularly or closely with children; or
- ✓ Behaved in a way that indicates they may not be suitable to work with children (including conduct outside the workplace that impacts suitability):

Immediate Escalation Protocol:

- ✓ The allegation must be reported immediately to **Kim, Head of Safeguarding** (or directly to the Chief Executive Officer / Board of Directors if the allegation involves the Head of Safeguarding).
- ✓ Within **24 hours**, the Lead DSL will notify the local authority **Local Authority Designated Officer (LADO)** to agree on next steps before initiating any internal investigation.
- ✓ Where warranted, platform permissions and system access will be suspended immediately to safeguard learners and preserve system audit trails.

Outside Employment, Conflicts of Interest, and Private Tuition

To prevent conflicts of interest and uphold safeguarding integrity:

- ✓ **Private Tutoring Prohibition:** Staff are strictly prohibited from providing private, paid, or voluntary tuition to any current or former EDClass learner, or to any pupil enrolled at an active EDClass commissioning school.

- ✓ **Secondary Employment:** Staff must declare any secondary employment, consultancy, directorships, or examination board roles in writing to the Senior Leadership Team. Secondary work must not interfere with scheduled teaching shifts or create a conflict of interest.
- ✓ **Intellectual Property:** All instructional content, video assets, curriculum pathways, slide decks, and code repositories developed during employment remain the exclusive intellectual property of EDClass Ltd.

Disciplinary Governance and Breach Escalation

This section establishes staff accountability, internal disciplinary procedures, and mandatory legal reporting to ensure online educators and operational staff do not compromise student safety, data integrity, or digital safeguarding boundaries.

Active Auditing and Monitoring Mechanisms

Compliance is continuously verified through multi-layered automated and supervisory checks:

- ✓ **Management Reviews and Lesson Observations:** Senior leaders and Lead DSLs periodically evaluate live instruction, pedagogical delivery, and pastoral boundaries.
- ✓ **Keystroke Audits and System Logs:** Digital inputs, system access events, and user activity are tracked to identify suspicious behaviour, unapproved software usage, or unauthorised searches.
- ✓ **Automated Alert Logs:** Real-time system flags automatically document and alert management to perimeter breaches, keyword violations, or protocol failures.

Minor Technical Breaches (Remedial Pathway)

Applies to low-risk, non-malicious procedural oversights that do not place a child in immediate harm:

- ✓ **Triggers:** Failing to engage system auto-lock when stepping away from a terminal, accidentally sharing an irrelevant browser tab during screen-share instruction, or using overly casual, informal language in chat that crosses minor professional communication standards.
- ✓ **Sanctions and Corrective Action:**
 - ✓ **Informal Coaching and Warning:** A targeted managerial conversation outlining the error.
 - ✓ **Mandatory Policy Refresher:** Compulsory re-training on acceptable use and digital boundary protocols.
 - ✓ **14-Day Re-Audit:** A strict two-week probationary check where the employee's logs, sessions, and screen activity are re-audited to confirm compliance.

Serious / Gross Misconduct (Dismissal Pathway)

Applies to deliberate actions that undermine platform security, compromise student welfare, or violate safeguarding standards:

- ✓ **Specific Gross Misconduct Triggers:**
 - ✓ **Off-Platform Communication:** Deliberately attempting to contact learners via personal phone numbers, personal email, gaming networks, or social media.
 - ✓ **Filter Circumvention:** Intentionally disabling, tampering with, or bypassing content filtering and keyword monitoring tools.
 - ✓ **Data Breaches and Credential Sharing:** Distributing identifiable student personal data or sharing platform login credentials.
 - ✓ **Suppression of Safeguarding Disclosures:** Failing to immediately log and report a known child protection disclosure or red-flag welfare indicator.
- ✓ **Sanctions:**
 - ✓ **Immediate Platform Suspension:** Instant revocation of all access to the system, databases, and student communication tools.
 - ✓ **Formal Disciplinary Hearing:** A rapid formal investigation conducted under employment regulations.
 - ✓ **Summary Dismissal:** Termination of employment with immediate effect without notice or pay in lieu of notice.

Mandatory Statutory Referrals (External Legal Duty)

When an employee's conduct harms a child or poses an ongoing risk of harm, EDClass has a statutory legal duty to make formal referrals, even if the individual resigns prior to the disciplinary hearing's conclusion:

- ✓ **Disclosure and Barring Service (DBS):** Formal notification sent to initiate barring proceedings, preventing the individual from working in regulated activity with children.
- ✓ **Teaching Regulation Agency (TRA):** Formal submission to the national regulatory body for teachers to evaluate professional misconduct and pursue lifetime teaching prohibition orders.
- ✓ **Statutory Timelines:** Filings must be submitted within strict legal deadlines to prevent an individual from moving to another educational institution unchecked.

Policy Integration and Document Review

This Code of Conduct and Acceptable Use Policy operates alongside the following corporate policies:

- ✓ Child Protection Policy
- ✓ Safeguarding Policy
- ✓ E-Safety, Filtering, and Monitoring Policy
- ✓ Relationships and Sex Education (RSE) Policy
- ✓ Special Educational Needs and Disabilities (SEND) Policy

- ✓ Whistleblowing Policy
- ✓ Data Protection Policy and Privacy Notice (GDPR/DPIA)
- ✓ Positive Behaviour, Repair, and Sanctions Policy
- ✓ Formal Complaints Policy

Staff Declaration and Operational Agreement

All staff members must review, sign, and date this policy upon appointment and annually thereafter following statutory review updates.

STAFF ACKNOWLEDGEMENT AND ACCEPTABLE USE AGREEMENT

I confirm that I have read, understood, and agree to abide by the EDClass Staff Code of Conduct and Acceptable Use Policy.

I recognise that all interactions on the EDClass platform are logged and recorded for safeguarding, quality assurance, and training purposes. I agree to uphold professional digital boundaries, protect learner personal data, and maintain high standards of teaching and child protection at all times.

Staff Member Full Name: _____

Role / Job Title: _____

Signature: _____

Date: _____