EDClass Ltd Data Protection Impact Assessment

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
This Data Protection Impact Assessment (DPIA) is tailored to the operations of **EDClass Ltd**, an alternative online education provider. It follows the standard UK ICO (Information Commissioner's Office) framework, focusing on the high-stakes nature of processing sensitive data for children and vulnerable learners. EDClass is a Department for Education Accredited Provider of Online Education and as such operates as an online alternative provision. There is a combined controller to controller operation with both The School/ The Academy / Local Authority (Commissioner) and EDClass Ltd. EDclass operates as the main educational facility for a child and young person and therefore control data when a CYP is being educated using the EDClass service. EDClass processes and controls **Special Category Data** (SEN, health, behavioural) on a **large scale** involving **vulnerable subjects** (children). The "eyes-on" live teaching and recording features also constitute systematic monitoring.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
To provide a granular view of the **EDClass Ltd** processing cycle, this section details the lifecycle of data from the initial referral to the final deletion, highlighting the technical and procedural safeguards at each stage. **How EDClass Collects the Data** Data is primarily sourced directly from the **commissioning educational institution** (The Data Controller). • **Automated Sync:** Integration with school Management Information Systems (MIS) like SIMS, Arbor, or Bromcom via **Wonde**. This ensures real-time accuracy.

- **Manual Input:** School administrators manually upload student profiles and safeguarding "Individual Learning Plans" (ILPs) via the secure EDClass portal.
- **User-Generated:** Students provide data through their interactions—completed coursework, chat logs with teachers, and live video/audio during "eyes-on" sessions.

How EDClass Use Data

The primary use is the delivery of **Alternative Provision (AP)** and distance learning.

- **Academic Tracking:** Monitoring progress against the National Curriculum.
- **Safeguarding:** Using "eyes-on" technology to verify student well-being and presence.
- **Reporting:** Providing schools/Local Authorities with attendance and attainment data for statutory DfE returns.

How EDClass Stores the Data

- **Location:** All data is hosted within the **UK** using **Amazon Web Services (AWS)**.
- **Security:** Data is encrypted at rest using **AES-256** and in transit via **TLS 1.2+**.
- **Architecture:** We utilise SQL databases with strict "Least Privilege" access—meaning staff only see the data necessary for their specific role.

How EDClass Deletes the Data

- **Retention Policy:** Data is held for the duration of the student's enrolment.
- **Triggered Deletion:** Upon contract termination or the student reaching the end of their key stage (e.g., Year 11), data is flagged for deletion.
- **Method:** Electronic records are cryptographically erased. Any physical backups (if applicable) are shredded. Following the **September 1st rule**, inactive accounts are purged unless a legal hold (safeguarding) is in place.

EDClass operates under a **"No Third-Party Sharing"** policy for commercial purposes. Data is only shared with:

1. **The Referrer:** Full transparency with the home school/LA.
2. **Safeguarding Partners:** If a "Life at Risk" or significant harm event occurs, data (logs/recordings) is shared with Social Care or the Police under **Schedule 1, Data Protection Act 2018**.
3. **Sub-processors:** Essential technical partners only (e.g., AWS for hosting, Wonde for MIS syncing), all of whom are bound by strict Data Processing Agreements (DPAs).

High-Risk Processing Activities

According to ICO guidelines, the following activities within EDClass are identified as **High Risk**, requiring the mitigations outlined in this DPIA:

1. **Systematic Monitoring:** The "eyes-on" webcam monitoring and tracking of student activity is a form of surveillance of vulnerable individuals.
2. **Sensitive Data at Scale:** Processing Special Category Data (Mental Health, SEN, Exclusion history) for thousands of minors.
3. **Inference-Based Decisions:** Using student data to flag "Safeguarding Alerts" or "Risk to Self" based on chat keywords or behaviour patterns.

4. **Data Combining:** Linking MIS data (demographics) with live behavioural data (platform engagement) to create a comprehensive profile of a child.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

EDClass processes a variety of data types to fulfil its educational and safeguarding mandates. This is categorised into **General Personal Data** and **Special Category Data**.

General Personal Data

- **Basic Identifiers:** Full name, preferred name, gender, and date of birth.
- **Contact/Logistics:** Year group, language, and school-assigned groups/classes.
- **Academic Records:** Predicted and achieved grades, lesson progress, completed coursework, and assessment answers.
- **Digital Footprint:** IP addresses, login timestamps, device information, and comprehensive "audit trails" of all platform interactions (clicks, actions, time spent learning).

Special Category & Sensitive Data

Due to the nature of Alternative Provision (AP), EDClass processes highly sensitive information, including:

- **Special Educational Needs (SEN):** Status, EHCP (Education, Health and Care Plan) details, and specific SEMH (Social, Emotional, and Mental Health) needs.
- **Health & Well-being:** Information regarding a child's mental health, "Child in Need" (CIN) or "Looked After Child" (LAC) status, and any physical health barriers to attendance.
- **Safeguarding Data:** Live video/audio streams, chat logs, and behavioural "alerts" or questionnaires designed to identify students at risk.
- **Criminal Offence Data:** While not a primary focus, data relating to **behavioural repair work** or "exclusion history" may include references to alleged or actual criminal activity or antisocial behaviour, which is handled under the strict "Substantial Public Interest" condition of the UK GDPR.

Volume and Frequency

- **How much data?** Profiles for thousands of students across **200+ schools and Multi-Academy Trusts (MATs)**. Each profile contains hundreds of data points ranging from attendance pings to full video lesson recordings.
- **How often?** * **Real-time:** Attendance, "eyes-on" visual monitoring, and chat interactions occur continuously during school hours (8:30 AM – 4:00 PM).
    - **Daily:** AM/PM registers are sent to schools and parents.
    - **Weekly:** Automated syncs via **Wonde** refresh MIS data (new students, leavers, updated grades) to ensure the platform remains accurate.

- **How many individuals?** The platform currently supports thousands of learners, primarily in the **Secondary (11–16)** age range, though it has the capacity for wider cohorts.
- **Geographical Area:** Processing is centred in the **United Kingdom**. All data is stored on **AWS servers located within the UK** to ensure compliance with UK GDPR and to minimise latency for live teaching.
- **Retention Period:**
    - **Standard:** Identifiable data is kept for the duration of the student's placement.
    - **Deletion Trigger:** Data is typically "soft deleted" (flagged for removal) once it is no longer required or upon written request from the school.
    - **Annual Purge:** A major data purge typically occurs on **September 1st** following the student's departure (e.g., end of Year 11) to ensure the system does not hold stale data.

The scope is considered "High Risk" under ICO criteria because:

1. **Vulnerable Subjects:** 100% of data subjects are children, many with SEN or SEMH challenges.
2. **Large Scale:** National-level processing across hundreds of UK institutions.
3. **Visual Monitoring:** Systematic use of webcams for safeguarding purposes.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

EDClass acts as a **Data Processor** for students (data subjects) who are referred by their school or Local Authority (the Data Controllers). The relationship is professional and educational, characterised by a duty of care.

- **Vulnerable Groups:** 100% of data subjects are **children**, a high percentage of whom belong to vulnerable subgroups, including those with **Special Educational Needs (SEN)**, **Mental Health difficulties (SEMH)**, or those at risk of exclusion.
- **Level of Control:** * **Students:** Have limited control over the *fact* of processing, as their education is often a statutory requirement. However, they can exercise rights (via their school) such as Subject Access Requests (SARs).
    - **Schools:** Retain high control, as they define which students are enrolled and can request "anonymous" account configurations where only non-identifiable IDs are used.

Public Expectations and Novelty

- **Expectations:** Parents and students expect data to be used for educational progress and safeguarding. The use of "eyes-on" webcam monitoring is expected within the specific context of **Alternative Provision (AP)** to ensure student safety when learning remotely.
- **Is it Novel?** While online learning is now mainstream, EDClass's specific "Virtual

Classroom" model—which integrates real-time safeguarding alerts, "eyes-on" tracking, and MIS syncing—is a specialised application of technology for high-risk cohorts.
- **Public Concerns:** Current public discourse often focuses on the "Digital Divide" and the ethics of **AI/Systematic Monitoring** of children. EDClass addresses this by ensuring human-led supervision (Qualified Teachers) rather than purely algorithmic monitoring.

State of Technology and Known Risks

The current state of EdTech (Education Technology) involves high levels of integration (APIs) and cloud-based storage. Known industry risks include:

- **"Zoom-bombing" / Unauthorised Entry:** Mitigated by EDClass using a proprietary, closed-loop system rather than public meeting links.
- **Phishing & Account Takeover:** Mitigated by strict password policies and encrypted data transfers.
- **Security Flaws:** EDClass uses modern **SALT encryption** and SQL firewalls to prevent similar exploits.

EDClass Ltd demonstrates its commitment to the highest security standards through rigorous external validation.

EDClass is certified to the latest **ISO 27001:2022** standard (Certificate No: CQ2022137). This international benchmark ensures:

- **Risk-Based Security:** Every part of the business undergoes regular threat assessments.
- **Continuous Improvement:** Security controls are not static but evolve with the threat landscape.
- **Management Commitment:** Information security is embedded in the organisational culture, not just the IT department.

EDClass holds the **Cyber Essentials** certification, confirming that its primary ICT defences are protected against the most common "commodity-based" cyber-attacks (e.g., hacking, phishing, and malware).

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The purposes of processing data within EDClass are centred on fulfilling the statutory and educational obligations of the **Data Controller** (the school or Local Authority) while providing a specialised, safe, and effective learning environment for the student.

1. What does EDClass want to achieve?

As a **Department for Education (DfE) Accredited Provider**, EDClass aims to remove the barriers that prevent students from accessing mainstream education. Their primary processing goals include:

- **Educational Continuity:** Providing a high-quality, digital curriculum (over 14,000 lessons) that mirrors the National Curriculum, ensuring students don't fall behind their peers during periods of absence.
- **Engagement and Reintegration:** Using personalised "learning pathways" to re-engage disengaged learners, with the ultimate goal of transitioning them back into mainstream school or preparing them for adulthood.
- **Robust Safeguarding:** Creating a "eyes-on" virtual environment where vulnerable learners are monitored via live video/audio, alert mechanisms, and session recording to ensure their physical and emotional safety.
- **Accurate Tracking:** Providing real-time data on attendance and attainment to the home school, ensuring they can fulfil their legal reporting duties.

2. What is the intended effect on individuals?

The processing is designed to have a **positive and protective** impact on the student:

- **Reduced Anxiety:** For students suffering from school refusal, bullying, or mental health issues, the online platform offers a "safe haven" where they can learn without the social pressures of a physical classroom.
- **Personalised Pace:** Students can work asynchronously or with 1:1 support, allowing them to bridge "knowledge gaps" without the embarrassment of falling behind in a group setting.
- **Empowerment and Voice:** Features like private chat and choice of communication (text vs. audio) empower students with SEN or communication difficulties to participate in a way that feels comfortable.
- **Improved Life Chances:** By preventing permanent exclusion and supporting GCSE completion, the processing aims to improve the student's long-term employability and well-being.

3. What are the benefits of the processing?

For EDClass (The Processor)

- **Service Delivery:** Enables them to fulfil their contractual obligations to schools and maintain their DfE accreditation.
- **Continuous Improvement:** Aggregated, anonymised data allows EDClass to refine their curriculum and platform accessibility features based on how students interact with the content.

For the School/Local Authority (The Controller)

- **Regulatory Compliance:** Provides the evidence needed for Ofsted inspections regarding alternative provision and safeguarding.
- **Reduced Workload:** Automated marking and attendance tracking save teachers hours of manual admin and lesson planning.
- **Cost-Efficiency:** Offers a scalable alternative to expensive 1:1 physical tutoring or high-cost off-site centres.

Broadly (Society & The Education System)

- **Reducing Exclusions:** By providing an effective "Internal Alternative Provision," the platform helps lower national exclusion rates.
- **Closing the Attainment Gap:** It ensures that vulnerable groups (SEND, Children in Care,

etc.) receive a comparable education to their peers, promoting social mobility.

- **Safeguarding at Scale:** Digital logs and recordings provide a level of oversight for off-site students that is often difficult to achieve through traditional "paper-based" home learning.

Key Takeaway: The processing is **not** for marketing or profiling; it is a strictly controlled educational intervention intended to protect a child's right to education and their physical safety while away from the school site.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

In line with Article 35(9) of the UK GDPR, a core component of a DPIA is consulting with relevant stakeholders. For EDClass, this process involves a multi-layered approach to ensure that those whose data is processed, and those who manage the technology, have a voice in the risk assessment.

1. Seeking Individuals' Views (Students & Parents)

The UK GDPR requires that you "seek the views of data subjects or their representatives" where appropriate.

- **When:** Consultation should occur during the "onboarding" or "admissions" phase, before a student begins using the platform.
- **How:** * **Parental Consent/Information Packs:** While the legal basis for schools is often "Public Task," schools should provide a **Transparency Letter** to parents explaining *why* EDClass is being used and inviting questions or concerns regarding privacy.
    - **Student Feedback Loops:** EDClass gathers views through user-experience (UX) surveys and feedback buttons within the portal. This allows students to report if they feel uncomfortable with features like the virtual classroom or webcam monitoring.
- **Justification for Not Consulting:** If a student is in a crisis situation (e.g., immediate risk of exclusion or severe safeguarding concern), formal consultation with the individual might be bypassed to prioritise their **Vital Interests** or the **Public Task** of education. This must be documented as a "proportionality" decision.

2. Internal Stakeholders (The EDClass Team)

Within the organisation, the DPIA is not a solo effort by the DPO. The following roles must be involved:

- **Data Protection Officer (DPO):** To provide independent oversight, monitor the DPIA's progress, and act as the point of contact for the ICO.
- **Product Development Manager:** Responsible for explaining how system upgrades or

new features (e.g., AI-driven learning tools) might change the data flow.

- **Designated Safeguarding Leads (DSLs):** Crucial for assessing the "Risk to Rights and Freedoms." They ensure that the data processed is sufficient to protect the child without being intrusive.
- **Board of Directors:** To provide the "sign-off" and ensure that any financial costs for risk mitigation (e.g., new encryption tools) are budgeted.

3. Consulting Processors & Sub-processors

EDClass (the Processor) must assist the School (the Controller), but EDClass also relies on its own sub-processors.

- **Assistance to the School:** Under **Article 28(3)(f)**, EDClass provides schools with their "Technical and Organisational Measures" document and GDPR Policy to help the school complete its own DPIA.
- **Sub-processor Consultation:** EDClass consults with **AWS (Amazon Web Services)** and **Wonde** regarding their infrastructure security.
    - *Example:* If AWS changes a data center location, EDClass must consult their compliance documentation to ensure it remains within the UK/EEA or has standard contractual clauses (SCCs) in place.

4. External Experts & Information Security

To ensure the DPIA is robust, EDClass involves external validation:

- **Information Security Experts:** EDClass undergoes annual audits for **ISO9001, 21001, 27001** and **Cyber Essentials**. The experts conducting these audits are consulted to identify technical vulnerabilities that must be recorded in the DPIA.
- **Legal Experts:** To ensure that the Data Processing Agreements (DPAs) are up to date with the latest UK GDPR case law and ICO guidance.
- **Ofsted/DfE Inspectors:** Through the **Online Education Accreditation Scheme (OEAS)**, external inspectors review EDClass's processes. Their feedback on safeguarding and data management is treated as a form of expert consultation for the DPIA.

Consultation Summary Table

Stakeholder	Method of Consultation	Focus Area
Parents/Students	Privacy Notices & Feedback Portals	Transparency and User Comfort
Internal DSLs	Weekly Safeguarding Reviews	Impact of monitoring on student privacy
AWS/Wonde	Review of SOC2 Reports/SLAs	Physical and Technical security of data
Cyber Essentials	External Security Audit	Vulnerability and Pen-testing results
The School (Controller)	Quarterly Account Reviews	Alignment with the School's own Data Policy

This DPIA is a **"living document."** If EDClass introduces a significant new technology (e.g., biometric login or automated facial recognition), a new round of consultation with all the above

stakeholders would be legally required.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

EDClass ensures compliance and proportionality by aligning its data practices with statutory educational requirements and strict security standards. As a processor, it operates under the direction of the school (the Controller), but it implements significant internal safeguards to ensure that data usage remains ethical, secure, and minimal.

1. Lawful Basis for Processing

The primary lawful basis for processing lies with the **Data Controller (the School)**. Under UK GDPR Article 6, this is typically:

- **Public Task:** Processing is necessary for the school to perform its official function of providing education and statutory alternative provision.
- **Legal Obligation:** Processing is required to fulfil attendance reporting and safeguarding duties (e.g., *Keeping Children Safe in Education*).
- **Special Category Data (Article 9):** EDClass processes health or SEN data under the condition of **Substantial Public Interest**, specifically for the purposes of safeguarding children and individuals at risk.

2. Effectiveness and Alternatives

- **Does it achieve the purpose?** Yes. By integrating MIS data (via Wonde), EDClass enables real-time attendance tracking and academic progress monitoring for students who cannot physically attend school. The 14,000+ lesson library and live tutor support directly facilitates educational continuity.
- **Is there another way?** While physical 1:1 tutoring is an alternative, it is often not scalable, lacks the same level of digital audit trails for safeguarding, and is significantly more expensive for schools. EDClass provides a middle ground that maintains a high level of "eyes-on" supervision digitally.

3. Preventing "Function Creep"

Function creep occurs when data is used for purposes beyond the original intent (e.g., marketing).

EDClass prevents this through:

- **Strict Access Controls:** System access is restricted to authorised personnel. Developers cannot access live student data unless a specific "Access Request" is granted and logged for troubleshooting.
- **Contractual Silos:** Data for School A is logically separated from School B. Data is never aggregated for commercial profiling or shared with third-party advertisers.
- **Limited Features:** The platform is a "closed-loop" system. Students cannot browse the open web or interact with unverified users, keeping data strictly within the educational context.

4. Data Quality and Minimisation

- **Minimisation:** EDClass only requests the data fields essential for a student's "seat"—name, year group, and necessary safeguarding flags. Schools can choose to keep accounts **anonymous** (using ID numbers instead of names) if they prefer higher levels of privacy.
- **Quality:** Data is synced daily via **Wonde**. This ensures that if a student's contact details or safeguarding status changes in the school's MIS, the EDClass record is updated within 24 hours, preventing the use of stale or inaccurate data.

5. Supporting Individual Rights

EDClass provides the technical tools to help schools fulfil student/parent rights:

- **Information Provided:** Individuals are informed via the school's Privacy Notice and EDClass's own transparency documentation provided during onboarding.
- **Right of Access/Rectification:** The platform allows school admins to pull "Activity Reports" or "Chat Logs" instantly to satisfy Subject Access Requests (SARs).
- **Right to Erasure:** EDClass implements a **"Soft Delete" policy**. Data is purged by September 1st following the student's departure from the platform, ensuring data is not held indefinitely.

6. Processor Compliance & International Transfers

- **Processor Oversight:** EDClass vets its sub-processors (like AWS and Wonde) through robust Data Processing Agreements (DPAs). They ensure all sub-processors maintain high security standards, such as ISO 27001 or Cyber Essentials.
- **International Transfers:** * **Data Residency:** EDClass primarily uses **AWS UK (London)** or **EEA (Dublin)** regions to ensure data stays within high-protection jurisdictions.
    - **Safeguards:** If any auxiliary data (like technical logs) must move outside the UK/EEA, it is protected by **Standard Contractual Clauses (SCCs)** or the **UK Addendum**, ensuring the data receives an equivalent level of protection as it would under UK law.

The intrusiveness of the processing (e.g., recording live lessons) is balanced against the high-risk nature of the students. Without these logs, the school could not guarantee the safety of a

vulnerable child learning off-site, making the processing **proportionate** to the safeguarding risk.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Sensitive Data Aggregation	Possible	Minimal	Low
Platform Accessibility	Possible	Minimal	Low
System Integration (MIS)	Possible	Minimal	Low
Internal Insider Threat	Possible	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Unauthorised Access to Safeguarding Logs: A hacker gains access to sensitive student case notes.	IP-restricted backend, 2FA for staff, SALT encryption on databases.	reduced	Low	Yes
Accidental Data Leak by Tutor: A tutor accidentally shares a screen showing another student's name.	Mandatory GDPR Level 2 training, "Screen-specific" sharing protocols, live DSL monitoring.	Reduced	Low	Yes
Sub-processor Breach (AWS): A vulnerability in the cloud hosting infrastructure.	Use of UK/EEA data centres, AWS Shield/WAF protection, Cyber Essentials certification.	Reduced	Low	Yes
Data Sync Error (Wonde):	Automated daily sync, manual verification of "high-risk" flags, data quality logs.	Reduced	Medium	Yes

Inaccurate data is pulled from the school MIS, leading to a safeguarding miss. **Function Creep:** Student data used for purposes other than education (e.g., marketing).	Contractual prohibitions in DPA, logical data separation by school, no third-party tracking.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA