School of Coding & AI

DATA MANAGEMENT AND EXTERNAL REPORTING POLICY

1. Introduction

1.1 Purpose

The policy sets out the framework through which the School of Coding & AI (SOC) ensures the integrity, accuracy, security, and responsible use of all data it manages as a delivery partner for UK universities and for internal organisational management and governance purposes. It sets out how SOC meets its obligations under OfS regulation, supports university partners in statutory reporting, and complies with UK data protection law. The policy ensures that data used for higher education delivery, widening participation, outreach, mobility programmes, research, and knowledge exchange is reliable, well-governed, and fit for regulatory scrutiny.

Activity and data covered by this policy ensures:

- Compliance with OfS Conditions B1-B5 (student outcomes), C1 (consumer protection), E2 (effective management);
- Support for university partners (statutory reporting lead) and other collaborators;
- Ensuring data quality for validation agreements, student protection, research integrity, and regulatory scrutiny;
- GDPR/UK DPA 2018 compliance as joint controller where applicable

1.2 Scope

This policy applies to all data generated/collected through SOC activities, including:

1.2.1 Student Data (via university partners or held by SOC)

- Personal identifiers (name, date of birth, contact details, unique learner numbers).
- Demographic characteristics (gender, ethnicity, disability, domicile, widening-participation indicators).
- Admissions and enrolment data (applications, offers, acceptances, enrolment status).
- Attendance, engagement, and participation records.
- Module and programme registrations.

- Assessment submissions, marks, grades, and progression decisions.
- Completion, withdrawal, suspension, and transfer data.
- Student outcomes (continuation, completion, attainment, progression to employment, or further study).
- Student feedback, complaints, and appeal data.
- Student support and reasonable adjustments records (where shared lawfully and contractually), including confidential records relating to welfare meetings.

1.2.2 Programme and Curriculum Data (via university partners)

- Programme specifications and validation documentation.
- Module descriptors, learning outcomes, schemes of work, assessment strategies, assessment briefs and student assessment work.
- Timetabling, delivery schedules, and teaching allocation.
- Changes to programme structure, delivery mode, or assessment.
- Data required for student protection planning and teach-out arrangements.

1.2.3 Regulatory and Quality Assurance Data (via university partners or held by SOC)

- Data supporting OfS Conditions B1–B5 (quality and student outcomes).
- Consumer protection information required for Condition C (course information, student contracts, relevant policies relating to the terms and conditions of the student contract, fees).
- Governance and management data required under Condition E2.
- Data for external quality reviews, audits, and partner oversight.
- Records of complaints, academic misconduct, appeals, and disciplinary outcomes.
- Data supporting access and participation, widening participation, and outreach evaluation.

1.2.4 Partnership and Contractual Data

- Data required in partnership agreements.
- Performance monitoring data for university partners.
- Data-sharing schedules, data-flow maps and standard operating procedures, and joint-controller/processor documentation, as appropriate.
- Records of compliance with contractual KPIs and reporting obligations.

1.2.5 Staff and Workforce Data

- Staff identifiers, roles, qualifications, recruitment and right-to-work information.
- Teaching and assessment allocations.
- Training and CPD records (including safeguarding, peer-observed teaching, PREVENT, data protection).
- Staff performance, workload, and deployment data relevant to programme delivery.

1.2.6 Outreach, Widening Participation (WP), and Impact Data

- Participant demographics and engagement records
- Activity design, delivery, and evaluation data
- Outcomes and impact measures for WP and outreach programmes.
- Data required for partner Access and Participation Plans (APPs).

1.2.7 Research and Knowledge-Exchange Data (via partners or held by SOC)

- Research project records, ethics approvals, and compliance documentation.
- Research participant data (where applicable and lawful) and other primary research data.
- Knowledge-exchange activity data, including industry partnerships and innovation outputs.
- Data supporting REF-related processes (where relevant to partner institutions).

1.2.8 Finance and Funding Data (via university partners)

- Tuition-fee and funding-related data supplied to university partners, where applicable.
- Records supporting SLC-related processes (where applicable).
- Financial data linked to programme delivery, subcontracting, and performance monitoring.
- Audit trails for payments, invoices, and contractual compliance.

1.2.9 Information Security and Governance Data

- Data-protection impact assessments (DPIAs).
- Records of data breaches, incidents, and remedial actions.
- Access-control logs and system-security records.
- Data-retention and disposal records.

1.2.10 Reporting Data for External Bodies (via university partners)

- HESA-related data (student, staff, finance, graduate outcomes).
- OfS regulatory data submissions.
- SLC-related data.
- Home Office compliance data for international students (if applicable).
- Data for professional, statutory, and regulatory bodies.

1.3 Definitions

Data: Any information created, collected, received, processed, stored, shared, or reported by SOC in the course of delivering higher-education programmes, outreach, research, or partnership activity. This includes personal data, operational data, academic records, financial information, and regulatory reporting data.

Personal Data: Information relating to an identified or identifiable individual, as defined by the UK GDPR and the Data Protection Act 2018. This includes names, contact details, demographic information, student records, staff data, and any other information that can directly or indirectly identify a person.

Special Category Data: A subset of personal data requiring additional protection due to its sensitivity, including data relating to health, ethnicity, disability, religion, sexual orientation, and other categories defined in the UK GDPR.

Data Controller: An organisation that determines the purposes and means of processing personal data. SOC may act as a controller or joint controller with university partners depending on contractual arrangements.

Joint Controller: Two or more organisations that jointly determine why and how personal data is processed. In some higher-education delivery arrangements, SOC and a university partner may share responsibility for specific data sets and reporting processes.

Data Processor: An organisation that processes personal data on behalf of a controller. SOC may act as a processor where a university partner retains full control of reporting and regulatory functions.

Data Processing: Any operation performed on data, whether automated or manual, including collection, storage, retrieval, analysis, sharing, reporting, retention, and deletion.

Data Quality: The accuracy, completeness, consistency, timeliness, and reliability of data used for operational, contractual, or regulatory purposes. High-quality data is essential for OfS compliance, statutory reporting, and partner assurance.

Regulatory Data: Data required to demonstrate compliance with OfS Conditions of Registration, including student outcomes, continuation, completion, consumer protection information, governance data, and any information needed external quality assurance or oversight.

Statutory Reporting: Mandatory reporting to regulators or government bodies, including the OfS, JISC, HESA, the Student Loans Company, the Home Office, or PSRBs. University partners remain the statutory reporting lead, with SOC providing accurate and timely data inputs.

Validation Data: Information required to support programme validation, quality assurance, academic oversight, and student protection planning by university partners.

Data Breach: Any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All breaches must be reported and managed in accordance with SOC's Data Breach Procedure.

Data Retention: The period for which data is stored before being securely deleted or anonymised, in line with legal, regulatory, and contractual requirements.

Data Subject: Any individual whose personal data is processed by SOC, including students, applicants, staff, volunteers, contractors, and outreach participants.

Information Security: The policies, controls, and technical measures used to protect data from unauthorised access, misuse, loss, or corruption.

Reporting Partner: A university or higher-education institution that retains statutory responsibility for external reporting and relies on SOC to provide accurate, timely, and compliant data for those submissions.

2. Policy Principles

SOC's approach to data management and reporting is guided by the following principles:

a. **Data integrity** — all data must be accurate, complete, timely, and consistent across systems and reporting cycles.
b. **Regulatory alignment** — data must meet the standards required by OfS Conditions B1–B5, C1, and E2, and support university partners in fulfilling their statutory reporting duties.
c. **Security and confidentiality** — data must be protected against unauthorised access, loss, misuse, or corruption, in line with GDPR and the UK Data Protection Act 2018, including encrypted storage access controls and annual penetration testing.

d. **Transparency and accountability** — roles, responsibilities, and data flows must be clearly defined, documented, and auditable; reflecting responsibilities and data management requirements set out in partnership agreements.
e. **Proportionality** — data collection and processing must be limited to what is necessary for operational, contractual, and regulatory purposes.
f. **Collaboration with partners** — SOC must work closely with university partners to ensure data quality, consistency, and compliance across joint processes.
g. **Continuous improvement** — data processes must be reviewed regularly to strengthen quality, reduce risk, and respond to changes in regulation or partner requirements.
h. **Formalised** — external data sharing must be formalised in agreements defining formats, timelines and responsibilities; including GDPR-compliant data management arrangements with partners and a Data Subject Access Request (DSAR) process with a one-month response time or sooner as specified in the partnership agreement.

3. Roles and Responsibilities

SOC is responsible for operating and maintaining systems, processes, and controls that ensure:

- High-quality data for all higher education delivery and reporting activities.
- Compliance with OfS regulatory expectations and university-partner requirements.
- Secure handling of personal and sensitive data.
- Clear documentation of data flows, validation checks, and reporting timelines.

The day-to-day responsibility for this sits with the Chief Operating Officer (COO), supported by the Director of Student Recruitment & Registry. Specific staff role-holders have the following responsibilities:

Role holder(s)	Responsibility
All SOC staff involved in creating, handling, or reporting data	• Follow this policy and associated procedures. • Complete mandatory data protection and data-quality training. • Report errors, inconsistencies, or risks as soon as they are identified. • Always protect confidential and personal data.

Data owners and managers	• Maintain accurate and up-to-date records within their area. • Implement validation checks and quality assurance processes. • Ensure data is processed in accordance with GDPR and partner agreements. • Escalate data quality or compliance risks promptly to the COO.
Senior Management Team	• Provide oversight of data governance and reporting processes. • Ensure adequate resources, training, and systems are in place. • Approve data-related policies, risk assessments, and quality assurance measures. • Ensure contractual obligations to university partners are met.
Principal	• Sign data sharing agreements. • Notify the Board and external agencies of data breaches.
Board of Directors	• Approval of this policy. • Review and approval of all OfS-required submissions. • Review the annual data quality and management report and any internal investigation and/or assurance reports related to this policy.

4. Data Quality Standards

Each type of data has a designated owner, who has responsibility for ensuring all necessary protocols are in place to ensure data quality and information security. Data quality checks are routinely carried out according to the following timetable unless otherwise specified in a partnership agreement or in cases where there is a data quality breach, where action is taken immediately.

Data Type	Data Owner	Frequency	Validation/Review process
Enquirer and applicant data	Director of Student, Recruitment & Records	At least weekly	Applicant profile data and recording of all interviews are reviewed by designated staff employed by University partners.
Student data relating to learning, teaching and student support	Heads of School Head of Student Services Program Leads	Except attendance data which is reviewed and acted upon on at least a weekly basis: Quarterly or termly depending on the partnership arrangements All data relating to registration, assessment and student progression are held on University systems and are subject to their review processes. Timescales required by University partners to support their external reporting duties.	Student Support team meetings Partnership Steering Group or equivalent. Regular review meetings with the University link tutors, programme managers and other staff supporting this work. Data quality and exceptions reports required by the university partner.

Programme and Curriculum data: held for the purposes of quality management and to support learning and teaching	Director of Learning and Teaching Heads of School Program Leads	Normally monthly within term-time.	Regular review meetings with the University link tutors, programme managers and other staff supporting this work.
Regulatory and Quality Assurance Data	Director of Learning and Teaching Heads of School Program Leads	Specified by University partners.	Partnership Steering Group (or equivalent) or task and finish group convened for a specific purpose.
Partnership and Contractual Data	COO	Specified by University partners or funders.	Partnership Steering Group (or equivalent).
Staff and Workforce Data	COO Director of Learning and Teaching. Heads of School. Program Leads. (for academic CVs, appraisals of teaching and related support staff, peer observed teaching)	Monthly Termly	Executive management group. Partnership Steering Group (or equivalent)
Outreach, Widening Participation, and Impact Data	Director of Student, Recruitment & Records	Termly	Executive management group or project review meeting for specific

			initiatives that are undertaken in partnership or externally funded.
Research and Knowledge-Exchange Data	Director of Research, Enterprise & Innovation	Termly or according to a different timescale specified by the partner or funder.	Executive management group or project review meeting for specific initiatives that are undertaken in partnership or externally funded.
Finance and Funding Data	Director of Student, Recruitment & Records (related to Higher Education) Chief Operating Officer (COO)	Monthly or according to timescales specified by the University partner. Monthly	Partnership Steering Group (or equivalent) or task and finish group convened for a specific purpose. Executive management group.
Information Security and Governance Data	Chief Operating Officer (COO)	Monthly	Executive management group.

5. Data Retention

The data retention schedule for each data type is prescribed by the relevant university partner, research organisation and/or funder. All other data are held according to the following timescales:

- Marketing and enquirer data: 2 years from last contact or consent withdrawal.
- Financial data: 7 years from transaction
- HR Data: 6 years post-employment (contracts); 1 year post-role (DBS).
- Staff and student feedback or testimonials: 5 years or consent expiry.
- Legal: 7 years from termination or the last payment.
- Technical and IT (including platform data): 2 years.

6. Procedure for Managing Data Breaches

SOC is committed to protecting personal data and responding promptly and effectively to any actual or suspected data breach. A data breach is any incident that results in the loss, unauthorised disclosure, or misuse of personal information.

6.1 Identifying and Reporting a Breach

Any member of staff or student who becomes aware of a potential data breach must report it immediately.

- Reports should be made to the Data Protection Officer (DPO).
- Do not attempt to investigate the breach yourself.
- Provide as much detail as possible, including what happened, when, and what data may be affected.

6.2 Initial Assessment

Once a report is received:

- The DPO (or nominee) will carry out an initial assessment to confirm whether a breach has occurred.
- Immediate steps may be taken to contain the incident, such as revoking access, recovering data, or securing systems.
- A risk assessment will be completed to determine the potential impact on individuals and on SOC.

6.3 Containment and Mitigation

If a breach is confirmed:

- The DPO will coordinate actions to contain the breach and prevent further loss or unauthorised access.
- Relevant teams (e.g., IT, HR, Registry) may be asked to support mitigation measures.
- Temporary restrictions or system changes may be put in place where necessary.

6.4 Notification

SOC will notify affected parties where required.

- If the breach presents a risk to individuals, SOC will notify the Information Commissioner's Office (ICO) within 72 hours.
- Individuals directly affected will be informed of:
    - what has happened

- what data is involved
- potential risks
- steps they can take to protect themselves
- what SOC is doing in response

- Notifications will be clear, timely and proportionate to the level of risk.

6.5 Investigation and Review

A formal investigation will be carried out to understand the cause and impact of the breach.

- The investigation will be led by the DPO or an appropriate senior manager.
- Findings will be documented, including:
  - how the breach occurred
  - what data was affected
  - who was impacted
  - actions taken
- Recommendations will be made to prevent recurrence, and responsible teams will be assigned actions.

6.6 Record-Keeping

SOC maintains a data breach log that records:

- all reported incidents
- assessments and decisions
- notifications made
- outcomes of investigations

This supports regulatory compliance and continuous improvement.

6.7 Learning and Improvement

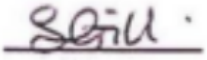
Following each breach:

- Relevant policies, procedures or training may be updated.
- Staff involved may receive additional guidance or support.
- Lessons learned will be shared with appropriate committees to strengthen organisational practice.

7. Training and Resources

- All relevant staff and Directors receive annual Cyber Security and Data Handling briefings, in addition to training provided by university partners.
- For further information, contact the Chief Operating Officer.

Name of provider: School of Coding & AI Ltd
Name of nominated accountable officer: Suki Gill
Designation: Principal

Signature: 
Date: 18th June 2026