INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-13 06:41 UTC

Student news - Student and alumni data has been compromised in a data security incident

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0167
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	University of Nottingham Student Record System
Published	2 days ago
Discovery Source	Serper

Executive Summary

The University of Nottingham has disclosed an unauthorized access incident affecting its student record system, with data belonging to current students and alumni confirmed as compromised. The full scope of exposed data fields has not been publicly confirmed, but student record systems typically hold names, contact details, dates of birth, and national identifiers. The institution faces immediate regulatory exposure under UK data protection law, reputational risk with prospective students, and potential harm to affected individuals through identity fraud or targeted social engineering.

Technical Analysis

The University of Nottingham confirmed unauthorized access to its student record system, as reported by ITV News (2026-06-10). No CVE is associated with this incident; it is an organizational breach rather than a disclosed software vulnerability. CWE-284 (Improper Access Control) and CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) are applicable weakness classifications. MITRE ATT&CK techniques observed or suspected in this class of incident include T1005 (Data from Local System), T1530 (Data from Cloud Storage), and T1078 (Valid Accounts). The attack vector, threat actor attribution, persistence mechanisms, and specific data fields exfiltrated have not been confirmed in available source material. No patch or vendor advisory applies; this is an access control and incident response matter.

Action Checklist

1. Step 1: Containment, Immediately audit and restrict access to the student record system; disable any accounts showing anomalous access patterns per NIST AC-2 (Account Management) and AC-3 (Access Enforcement); isolate affected system segments if unauthorized access pathways remain active.
2. Step 2: Detection, Review authentication logs and access audit records for anomalous login times, geographic anomalies, bulk data export events, and service account activity against the student record system; apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs); look for indicators consistent with T1078 (valid account misuse) and T1530 (cloud storage access).
3. Step 3: Eradication, Rotate all credentials with access to the student record system per NIST AC-2 (Credential Rotation); enforce MFA on all administrative and remote access paths per NIST AC-17 (Remote Access) and CIS 6.3, 6.4, 6.5; review and tighten access control lists per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists).
4. Step 4: Recovery, Validate that unauthorized access pathways are closed; confirm audit logging is fully operational per NIST AU-2 and AU-12 before restoring normal operations; monitor for re-entry attempts or secondary exfiltration; notify affected individuals and the UK Information Commissioner's Office within statutory timeframes.
5. Step 5: Post-Incident, Conduct a formal access control review against NIST AC-2, AC-3, and AC-6 to identify over-provisioned accounts; implement local account monitoring and user account permissions controls; update the incident response playbook to address student record system breach scenarios; review data minimization and retention practices per CIS 3.2 and 3.4.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to institutional leadership, legal counsel, and the UK ICO if confirmed exfiltration scope exceeds 500 data subjects, if national identifiers (National Insurance numbers, passport data) are confirmed among exposed fields, if evidence of ongoing unauthorized access is detected after initial containment, or if the 72-hour UK GDPR Article 33 ICO notification window is at risk of being breached.
Recovery Notes	Before returning the student record system to normal operations, independently verify via firewall logs and application session tables that all unauthorized access pathways identified during detection are closed, and confirm that MFA enforcement and new credential policies are active and tested end-to-end. Maintain elevated monitoring — specifically alerting on off-hours logins, bulk query events exceeding 100 records per session, and any new service account activity — for a minimum of 30 days post-containment, given that threat actors with prior valid-account access often attempt re-entry after defensive activity subsides. Coordinate with the University's data protection officer to ensure affected students and alumni receive timely notification letters that accurately reflect the confirmed scope of exposed data fields, and preserve all incident documentation for potential ICO investigation.

Forensic Artifacts	Student record system application-layer audit logs: session records showing query patterns, record counts retrieved per session, and export/download events — bulk retrieval of student records (names, DOBs, national identifiers) in a single session is the primary exfiltration indicator for this breach type | Identity provider / SSO authentication logs (Microsoft Entra ID sign-in logs or Shibboleth IdP audit logs) scoped to the student record system's service provider entity, covering at minimum 90 days pre-disclosure — these reveal the initial access vector, credential source, and session history for the unauthorized actor | Database server query logs (SQL Server Extended Events / default trace, or PostgreSQL pg_log) filtered for large-row-count SELECT statements against student, alumni, or contact tables — the query pattern distinguishes administrative access from bulk harvesting | VPN or remote access gateway session logs correlating source IP geolocation, session duration, and authenticated username to student record system access events — geographic anomalies or impossible travel indicators point to credential compromise rather than insider threat | Windows Security Event Log Event IDs 4624 (successful logon), 4648 (explicit credential use), 4672 (special privilege assigned), and 4776 (credential validation) on the student record system host and any jump hosts, providing the authentication chain from initial access through lateral movement to the record system

Per-Action IR Details

Step 1: Containment — Immediately audit and restrict access to the student record system; disable any accounts showing anomalous access patterns per NIST AC-2 (Account Management) and AC-3 (Access Enforcement); isolate affected system segments if unauthorized access pathways remain active.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-12 (Session Termination), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run 'Get-ADUser -Filter * -Properties LastLogonDate,Enabled | Where-Object {$_.LastLogonDate -gt (Get-Date).AddDays(-1)}' to surface recently active accounts, cross-reference against your staff roster to identify orphaned or unexpected accounts; use osquery ('SELECT * FROM logged_in_users;') on the student record system host to enumerate live sessions before revoking; block external egress from the student record system at the perimeter firewall using an explicit deny-all outbound rule scoped to the hosting subnet.

Evidence: BEFORE disabling accounts or isolating segments, capture: (1) active authenticated sessions from the student record system's application server logs (typically located at /var/log/app/ or IIS logs at C:\inetpub\logs\LogFiles\) including session tokens, source IPs, and timestamps; (2) live network connections via 'netstat -ano' or 'Get-NetTCPConnection' on the application server to identify active or recently closed connections to the student record database; (3) OS-level authentication records — Windows Security Event Log Event ID 4624 (successful logon) and 4634 (logoff) filtered to the student record system's hostname, and Linux /var/log/auth.log or /var/log/secure for the same window. Volatile session state is destroyed the moment accounts are disabled or the host is isolated.

Step 2: Detection — Review authentication logs and access audit records for anomalous login times, geographic anomalies, bulk data export events, and service account activity against the student record system; apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs); look for indicators consistent with T1078 (valid account misuse) and T1530 (cloud storage access).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Parse IIS or Apache access logs with 'grep -E "(SELECT|EXPORT|download|bulk|report)" /var/log/apache2/access.log' to surface bulk data retrieval URIs; for Windows environments, run 'Get-WinEvent -LogName Security -FilterXPath "*[System[EventID=4648 or EventID=4672 or EventID=4776]]"' to isolate explicit credential use and privilege escalation events; deploy a Sigma rule targeting large HTTP response sizes (>1MB) from the student record system's web endpoint as a proxy for bulk export activity; correlate login timestamps against off-hours windows (nights, weekends, UK public holidays) which are high-signal for unauthorized access in academic environments.

Evidence: No live-state alteration occurs in this detection step, so order-of-volatility sequencing is not the primary concern here; however, analysts must preserve log integrity before any downstream containment actions destroy context. Capture and hash (SHA-256) the following before proceeding: (1) student record system application-layer audit logs showing record queries, export events, and pagination patterns — bulk access of >500 records in a single session is a key indicator in a student record compromise; (2) identity provider or SSO logs (e.g., Microsoft Entra ID sign-in logs, Shibboleth IdP logs) filtered to the student record system's service provider entity for the 30 days preceding disclosure; (3) database query logs (SQL Server: default trace or Extended Events; PostgreSQL: pg_log) showing SELECT * or large row-count queries against student tables; (4) VPN or remote access gateway logs showing source geolocation and session duration for accounts that accessed the student record system.

Step 3: Eradication — Rotate all credentials with access to the student record system per D3-CRO (Credential Rotation); enforce MFA on all administrative and remote access paths per NIST AC-17 (Remote Access) and CIS 6.3, 6.4, 6.5; review and tighten access control lists per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 3.3 (Configure Data Access Control Lists)

Compensating: For MFA enforcement without enterprise tooling, configure Windows Hello for Business via Group Policy (Computer Configuration > Windows Settings > Security Settings > Public Key Policies) for admin accounts; for Linux SSH, enforce TOTP using libpam-google-authenticator and set 'AuthenticationMethods publickey,keyboard-interactive' in sshd_config; rotate service account passwords using 'Set-ADAccountPassword -Identity -NewPassword (ConvertTo-SecureString -AsPlainText "" -Force) -Reset' and immediately invalidate Kerberos tickets with 'klist purge' on affected hosts; audit ACLs on the student record database with 'SHOW GRANTS FOR "@";' (MySQL) or '\du' (PostgreSQL) and remove any accounts with SELECT rights on student tables that lack a documented business need.

Evidence: BEFORE rotating credentials or modifying ACLs, capture: (1) a full export of current account permissions on the student record system database ('SHOW GRANTS' / 'pg_roles' / SQL Server sys.database_permissions) as a baseline for post-eradication comparison and audit trail; (2) all active Kerberos TGTs and service tickets on the student record system host ('klist' output, Windows Security Event ID 4768/4769) — rotating passwords without invalidating existing tickets leaves live sessions active; (3) any scheduled task or cron job definitions that invoke service account credentials against the student record system (Windows: 'Get-ScheduledTask | Where-Object {$_.Principal.UserId -like "*svc*"}'; Linux: 'crontab -l -u ') — these persist after password rotation and must be updated or they will break and generate detectable error events.

Step 4: Recovery — Validate that unauthorized access pathways are closed; confirm audit logging is fully operational per NIST AU-2 and AU-12 before restoring normal operations; monitor for re-entry attempts or secondary exfiltration; notify affected individuals and the UK Information Commissioner's Office within statutory timeframes.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-9 (Protection Of Audit Information), CIS 8.2 (Collect Audit Logs)

Compensating: Verify audit logging is operational by generating a known test event (e.g., a deliberate failed login against the student record system) and confirming it appears in both the application log and any forwarding destination within 60 seconds; use 'auditctl -l' (Linux) or 'AuditPol /get /category:*' (Windows) to confirm audit policy is active; deploy a free Wazuh agent on the student record system host to forward logs to a central Wazuh manager for re-entry detection without a commercial SIEM; for ICO notification tracking, document breach discovery date, affected data categories, and estimated number of data subjects — UK GDPR Article 33 mandates ICO notification within 72 hours of the organization becoming aware, and Article 34 requires communication to affected individuals without undue delay when high risk to rights and freedoms is present.

Evidence: Before restoring normal operations, confirm: (1) all previously identified malicious or anomalous sessions are absent from 'Get-NetTCPConnection' and application session tables; (2) firewall egress rules blocking the student record system's subnet from unauthorized external destinations are confirmed in the firewall ruleset and tested; (3) a clean baseline snapshot (file integrity hash via AIDE or Windows SFC /scannow) of the student record system's application binaries and configuration files is captured and stored off-system, providing a reference point for detecting re-compromise during the monitoring window. The 72-hour ICO notification deadline is a hard regulatory trigger — document the exact timestamp breach awareness was confirmed and work backward to validate compliance.

Step 5: Post-Incident — Conduct a formal access control review against NIST AC-2, AC-3, and AC-6 to identify over-provisioned accounts; implement D3-LAM (Local Account Monitoring) and D3-UAP (User Account Permissions) controls; update the incident response playbook to address student record system breach scenarios; review data minimization and retention practices per CIS 3.2 and 3.4.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-11 (Audit Record Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run a quarterly access recertification using a simple spreadsheet cross-referencing AD group membership ('Get-ADGroupMember -Identity "StudentRecordSystem_ReadWrite" -Recursive') against HR active-employee and active-student lists — accounts not matching an active identity should be disabled per CIS 5.3; use osquery scheduled queries ('SELECT * FROM users; SELECT * FROM user_groups;') to maintain a live local account inventory on the student record system host; for data minimization, query the student record database for fields populated with national identifiers (NI numbers, passport numbers) and confirm each field has a documented retention schedule tied to the data inventory required by CIS 3.2.

Evidence: Post-incident artifacts to preserve for lessons-learned and regulatory evidence packages: (1) the complete authentication log corpus covering the breach window, retained per NIST AU-11 requirements and UK GDPR Article 30 (Records of Processing Activities) obligations; (2) the access control baseline captured during eradication (Step 3), used to demonstrate what over-provisioned accounts existed at time of breach; (3) a written timeline of breach discovery, containment actions, and ICO notification with exact timestamps, which constitutes the organization's Article 33(3)(d) documentation obligation; (4) the output of the formal access control review (account list, permissions matrix, and remediation actions taken) as evidence of post-incident control improvement for any future ICO investigation.

Detection Guidance

Query authentication and access logs on the student record system for: bulk record retrieval events in short time windows; logins from unusual IP ranges or geolocations inconsistent with staff and student populations; service or API accounts accessing data volumes outside baseline; after-hours administrative access. Apply NIST AU-6 (Audit Record Review) and AU-3 (Content of Audit Records) to ensure logs capture who accessed what, when, and from where. MITRE T1078 (Valid Accounts) suggests reviewing for credential misuse rather than novel malware; focus on legitimate-looking access with anomalous scope or timing. T1005 and T1530 suggest examining file export, download, and cloud storage access logs. No specific IOC hashes, IPs, or domains have

been confirmed in available source material for this incident.

Framework Mappings

MITRE-ATTACK

- **T1005** — Data from Local System
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1530	Data from Cloud Storage	Collection

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://www.nottingham.ac.uk/currentstudents/news/student-and-alumn...	T3
Penn Data Breach Involves Decades of Student and Alumni ...	https://www.nytimes.com/2025/11/04/us/penn-data-breach-donors-stude...	T2
Hackers target online education system #canvas putting ... - Instagram	https://www.instagram.com/reel/DYEB16ytMIM/?hl=en	T3
University of Nottingham student and alumni data accessed in hack ...	https://www.itv.com/news/central/2026-06-10/university-of-nottingha...	T3
My SSN was exposed in a breach at Columbia—a school I have no ...	https://www.reddit.com/r/technology/comments/1twom0y/my_ssn_was_exp...	T3

Generated 2026-06-13 06:41 UTC by TJS Security Command Center