

E-SAFETY POLICY (DATA PROTECTION AND DIGITAL PLATFORM USE)

Policy Owner	Head of Assessments & Data
Approved by	Ms Sapna Changrani (Head of School)
Effective Date	July 2026
Next Review Due	July 2027
Circulation	Staff, Students, Parents, Governors, Vendors

1. PURPOSE

Dubai Scholars Private School (DS) recognises its responsibility to protect personal data and ensure the safe, ethical, and secure use of digital platforms used for teaching, learning, communication, administration, safeguarding, and assessment. This policy applies to all staff, students, parents, contractors, governors, volunteers, consultants, and third-party service providers, and has been developed with reference to UAE Federal Decree-Law No. 45 of 2021 (PDPL), the UAE Cybercrime Law, and KHDA regulations and guidance.

2. SCOPE

This policy applies to all personal and sensitive information processed by Dubai Scholars — including admissions, academic, behaviour, SEND, and medical records for students; contact, financial, and consent records for parents; and recruitment, payroll, and performance records for employees — regardless of whether it is stored digitally, on cloud systems, on school devices, or in paper format.

3. DATA PROTECTION PRINCIPLES

Dubai Scholars will ensure that all personal data is lawfully processed, fair and transparent, purpose-limited, accurate, secure, and retained appropriately.

4. DIGITAL PLATFORM USE

Dubai Scholars uses a range of digital platforms to support learning and school operations, including Toddle, Orison/MIS systems, Microsoft 365, and approved AI tools. No digital platform may be used with students unless approved by the SLT, reviewed by the Head of Assessments & Data for data protection and safeguarding compliance, and approved by the IT Department. All vendors must demonstrate compliance with UAE data protection requirements, appropriate security controls, and student safeguarding protections.

5. STAFF RESPONSIBILITIES

Staff must access only information required for their role, maintain confidentiality, use only approved school systems, and comply with the Dubai Scholars AI Policy — including not entering identifiable student information into public AI systems, and ensuring human oversight remains in place for educational decisions.

6. STUDENT RESPONSIBILITIES

Students must use school platforms responsibly, protect login credentials, respect the privacy of others, and follow acceptable use expectations.



Students Must NOT:

Share passwords, access another user's account, record or distribute personal information without permission, upload inappropriate content, or use AI tools to gain unfair academic advantage. Misuse may result in restricted access, behaviour sanctions, safeguarding investigation, or disciplinary action.

7. PARENT RESPONSIBILITIES

Parents and guardians are expected to keep login credentials secure, use school platforms responsibly, protect confidential school communications, and notify the school of suspected account misuse.

8. DATA SHARING

Dubai Scholars may share information only when there is a legitimate basis and with Head of School approval — for educationally necessary purposes, legally required purposes (e.g. with KHDA, the Ministry of Education, or law enforcement), or safeguarding purposes — always following the principle of minimum necessary disclosure.

9. INFORMATION SECURITY

The school will maintain reasonable technical controls (multi-factor authentication where possible, secure passwords, encryption, firewall protection) and organisational controls (staff training, acceptable use agreements, vendor review, incident response procedures).

10. CCTV, PHOTOGRAPHY AND DIGITAL MEDIA

Dubai Scholars uses CCTV for safety, security, safeguarding, and site management. Student photographs, videos, and recordings may only be used with appropriate consent where required, for legitimate educational or promotional purposes.

11. DATA BREACHES AND INCIDENT REPORTING

Any suspected breach must be reported immediately to the Line Manager, IT Department, Head of Assessments & Data, and, where relevant, the Designated Safeguarding Lead. The school will investigate incidents promptly, mitigate risks, and notify relevant authorities where required.

12. PUPIL-FACING INTERNET CONDUCT AND BYOD

- Mobile phones are not permitted for use during the school day; where a phone is brought to school with permission, it must remain switched off and stored in a bag or locker, and a phone seen in use may be confiscated and returned at the end of the day.

- The school's approach to Bring Your Own Device (BYOD) is guided by clear e-safety principles: an Acceptable Use Agreement for all users, differentiated network access by user type, and regular audits and monitoring of personal device use on school networks.
- Cyberbullying incidents are addressed in connection with the school's Behaviour (Restorative) Policy: an identified incident is initially investigated and reported as Stage 1, and escalated to Stage 3 where confirmed as sustained bullying.
- Students must not divulge personal information about themselves or others online, must never upload images of themselves or others without permission, and must immediately inform a trusted adult if they receive an inappropriate or uncomfortable message.
- Students must not attempt to bypass school network filtering or restrictions using personal mobile data or a VPN while on school premises.

13. MONITORING, COMPLIANCE AND GOVERNANCE

The school will regularly review platform usage, access permissions, vendor compliance, security controls, and data handling practices, including system audits, access reviews, security testing, staff training records, and incident reviews.

14. CONTACT INFORMATION

Questions relating to this policy should be directed to the Head of Assessments & Data. For safeguarding concerns, individuals should contact the Designated Safeguarding Lead.

15. POLICY REVIEW

 **This policy will be reviewed annually, or sooner if required, to reflect operational needs, changes in legislation, or updated guidance from the KHDA**