BELVEDERE
INTERNATIONAL SCHOOL

STUDENT DIGITAL SYSTEMS AND TECHNOLOGY POLICY

2026-2027

Document No.	**POL-AC-012**
Revision No.	**002**
Issue Date	**14 September 2026**
Effective Date	**16 September 2026**
Review Date:	**09 September 2026**
Next Review Date:	**09 September 2027**

Approvals:			
Principal	**Mr. Ismat Daou**		
Signature		Date:	10/9/26
BIS Board of Governors	**Dr. Naim Alradi**		
Signature		Date:	12/9/26

1. Purpose, Scope and Definitions

This policy sets the rules for how Belvedere International School students use school-managed digital systems, and how the school protects the data held in them.

Scope. It applies to all enrolled students, and to parents, teachers and staff who administer or interact with the systems below: ClassDojo, Google Classroom, the network firewall, school email, campus WiFi, student Google accounts and the Mograsys Student Information System (SIS).

Definitions.

- **School systems:** any platform, account, device or network provided or managed by the school.
- **Student data:** any information that identifies a student, including name, grades, attendance, photos, messages and login details.
- **IT Manager:** the staff member(s) responsible for managing accounts, network and platform settings.
- **IT Manager:** the staff member accountable for a given system's data (for example, the Registrar for Mograsys).

Principles. Systems are for learning and school communication. Students get the minimum access they need. Student data is collected only for school purposes and is protected from misuse.

2. ClassDojo

ClassDojo is used for positive behaviour recognition, class updates and teacher–parent communication, and is not a general social platform.

- **Accounts:** Teachers create class accounts. Parents join using the school-issued invite code or QR link only.
- **Content:** Teachers may post behaviour points, class announcements and learning updates. Student photos or videos are posted only where parental media consent is on file.

- **Points and feedback:** Points reward behaviour and effort. They must be applied consistently and must never be used to shame or publicly compare students.

- **Communication:** Parent–teacher messages are for school matters, during reasonable hours (7:00 am – 5:00 pm, Sunday to Thursday unless urgent). Staff do not use personal accounts or numbers for ClassDojo.

- **Student conduct:** Students must not share class or parent login details, or screenshot and redistribute other children's data.

- **Privacy:** Only the minimum student information needed is entered. Portfolios and class stories are visible only to the class community.

- **Removal:** At year end or on withdrawal, the teacher archives or removes the student profile, and the IT Administrator confirms deletion on request.

3. Classroom (Google Classroom)

Google Classroom is the school's main platform for assignments, resources and feedback.

- **Access:** Students join classes only with their school Google account. Teachers own and manage all classes; students cannot create classes.

- **Assignments:** Students submit work by the stated deadline in the stated format. Late submissions follow the teacher's published rules.

- **Academic integrity:** Work submitted must be the student's own. Copying, sharing answers or using unapproved AI tools to complete graded work is academic misconduct.

- **Respectful conduct:** Class comments and the stream are for learning. Bullying, inappropriate language, off-topic chat and sharing personal information are not allowed.

- **Files and links:** Students must not share class materials, meeting links or Google Meet codes outside the class.

- **Live lessons:** Students join with their real name, follow teacher instructions on camera and microphone, and must not record lessons without permission.

- **Teacher oversight:** Teachers may review, mute or remove comments and content, and report concerns to the school leadership.

- **Archiving:** Classes are archived at the end of the academic year. Students keep access to their own work through their account while enrolled.

4. Firewall and Web Filtering

The school firewall protects students and the network by filtering web traffic on all campus connections.

- **Filtering:** Content is blocked by category, including adult content, gambling, violence, drugs, malware and phishing, proxy/VPN services, and unapproved file-sharing.

- **Age-based profiles:** Students are filtered more strictly than staff, and younger students more strictly than older students.

- **Bypass prohibited:** Students must not use VPNs, proxies, hotspots, DNS changes or any tool to avoid the firewall.

- **Monitoring:** Web activity on the school network is logged. Logs are reviewed only by authorised staff for safeguarding and security, and are not shared outside the school except where required by law.

- **Unblock requests:** If a site needed for learning is blocked, a teacher submits a request to the IT Administrator. Requests are reviewed within 2 working days.

- **Reporting:** Students must tell a teacher at once if they reach inappropriate content or receive a suspicious link.

- **Changes:** Only the IT Administrator may change firewall rules, and each change is recorded with the date and reason.

5. Email

School email is provided for learning and communication with teachers and school staff.

- **Ownership:** Student email addresses belong to the school and are issued for the period of enrolment.
- **Permitted use:** Contacting teachers, submitting work, receiving school notices and using approved educational services.
- **Not permitted:** Chain mail, spam, bullying or threatening messages, sharing inappropriate content, sending large or unsafe attachments, and signing up to non-educational services.
- **Etiquette:** Messages use a clear subject, respectful language and the student's real name. Students communicate with staff only through school email.
- **External senders:** Younger students can send and receive email only within the school domain unless a teacher requests otherwise.
- **Phishing:** Students must not open suspicious links or attachments, and must report them to a teacher or the IT Administrator.
- **Monitoring:** Email is filtered for spam, malware and harmful content. The school may access a student's mailbox where there is a safeguarding or serious conduct concern, with approval from school leadership.
- **Retention:** Mailboxes are suspended on withdrawal or graduation and deleted after the retention period in Section 7.

6. WiFi Access on Campus (Student Policy)

Campus WiFi is a privilege for educational use and is available to students only as set out below.

- **Who may connect:** Students connect to the designated student network only, using their own school Google account. Student devices are not allowed on the staff network.

- **Devices:** Only school-approved devices, or personal devices approved under the school's device programme, may connect. Each student may register a limited number of devices with the IT Administrator.

- **Mobile phones:** Phones follow the school's mobile phone rules and may be connected only when a teacher permits it for a lesson.

- **Credentials:** Passwords and WiFi access details must not be shared. Students are responsible for activity under their account.

- **Prohibited:** Hotspots or routers, VPNs, hacking or scanning tools, torrenting, streaming or gaming not set by a teacher, and attempts to access other users' devices or accounts.

- **Bandwidth:** The school may limit speeds or block high-use services to protect learning.

- **Access times:** Access is available during school hours and approved activities, and may be switched off at other times.

- **Responsibility:** The school is not liable for loss, damage or theft of personal devices, or for personal data on them.

- **Suspension:** Access may be suspended immediately for a suspected security risk or a breach of this policy.

7. Student Google Account

Each student receives one school Google Workspace account, which gives access to email, Classroom, Drive and other approved apps.

- **Creation:** The IT Administrator creates accounts from enrolment data in Mograsys. Accounts follow the school's standard naming format.

- **First login:** Students change their temporary password at first sign-in. Passwords must be at least 12 characters and must not be shared, written down or reused elsewhere.

- **Security:** Two-step verification is required for older students and recommended for all. Students sign out on shared devices.

- **Personal use:** The account must not be used to sign up for personal social media, games or non-school services.

- **Drive and sharing:** Files are shared only with teachers and classmates for school tasks. Public ("anyone with the link") sharing is turned off for student accounts.

- **Apps and add-ons:** Only apps approved by the IT Administrator may be installed or connected.

- **Lost or compromised accounts:** Students report these to the IT Administrator immediately. The password is reset and activity is reviewed.

- **Ownership and monitoring:** The account and its content belong to the school and may be reviewed for safeguarding or security reasons.

Account lifecycle and retention

Event	Action	Timing
Withdrawal or transfer	Account suspended	Last day of attendance
Graduation	Student may export own files	30 days before closure
Suspended account	Data and mailbox deleted	90 days after suspension
Year-end promotion	Account moves to the new class group	Before term start

8. Mograsys SIS Data

Mograsys holds the school's official student records, and is the source for accounts in other systems.

- **Data held:** Student and parent contact details, enrolment, attendance, timetables, grades and reports, behaviour and health notes, and fee information.

- **Purpose:** Data is used only for teaching, administration, safeguarding, reporting to authorities and communicating with parents.

- **Access by role:** Access is given on a need-to-know basis, as shown below. Staff may not view records outside their duties.

Role	Access
Registrar and admissions	Full student record
Teachers	Own classes: attendance, grades, contacts
Finance	Fee and payment data only
Leadership	Reports and records as needed
IT Administrator	System administration, not routine record content
Parents	Own child's information through the parent portal

- **Accounts:** Each user has a personal login. Shared logins are not allowed and passwords must meet the account password standard in Section 7.

- **Accuracy:** Data is entered promptly. Parents report changes in contact details, and corrections are made by the Registrar.

- **Sharing and export:** Data is shared outside the school only where required by law, the education authority or with parent consent. Exports and printouts are kept secure and destroyed when no longer needed. Data is never sent over personal email or messaging apps.

- **Audit:** Access and changes are logged. The Data Owner reviews user access each term and removes leavers immediately.

- **Breaches:** Any suspected loss or misuse of data is reported to the IT Administrator and school leadership on the same day.

- **Retention:** Records are kept for the period required by law and school regulations, then securely deleted or archived.

9. Violations, Review and Acknowledgement

Breaches are handled in line with the school's behaviour policy, and the response depends on how serious the breach is.

Level	Examples	Possible response
Minor	Off-task use, sharing a class link	Verbal warning, parent informed
Moderate	Bypassing the firewall, using another student's account	Access restricted, parents called in, detention
Serious	Bullying online, hacking, accessing or leaking student data	Account suspended, formal disciplinary action, possible report to authorities

Review. The IT Administrator and school leadership review this policy every year, or sooner after a major incident or a change in law or systems.

Acknowledgement. Parents and students sign the acknowledgement below at admission and when the policy is updated.

I have read and understood the Student Digital Systems & Technology Policy of Belvedere International School and agree to follow it.

Student name	**Class**	**Parent/guardian name**	**Signature**	**Date**