



**The Bay
Academy**

Policy No.: TBA014

**SCHOOL DATA
MANAGEMENT POLICY**

1. PURPOSE OF THE POLICY

- 1.1. The purpose of this policy is to ensure that all data, electronic communication, social media usage, and assessment records at The Bay Academy ("**the School**") are managed responsibly, securely, and in accordance with legal and ethical standards. This policy outlines the responsibilities of employees regarding the use of school IT systems, digital devices, internet, social media, and the management of learner records.

2. SCOPE

- 2.1. This policy applies to all employees of The Bay Academy, including teaching staff, administrative staff, and management, when handling:
 - 2.1.1. School computers, networks, and other electronic devices;
 - 2.1.2. internet and email communications;
 - 2.1.3. social media platforms and digital messaging applications; and
 - 2.1.4. learner assessment records, attendance, and progression data.
3. Computers, electronic devices, and communication systems provided by the School are to be used solely for educational and business purposes.
4. Personal use of School equipment requires prior authorisation and may incur reimbursement. Excessive personal use may result in disciplinary action.
5. Employees must operate all electronic equipment safely, properly, and in accordance with IT security policies.
6. Any unauthorised, harmful, or commercial use of School equipment is considered misconduct. This includes hacking, unauthorised access, or damaging systems.
7. The School reserves the right to monitor and review the use of all electronic devices, emails, internet usage, and other digital communications. Employees consent to such monitoring as a condition of employment.
8. Employees must comply with the School's Code of Conduct and other relevant policies when using electronic systems.
9. Misuse of electronic equipment or online communications, even outside work hours or on personal devices, which negatively impacts the School, may result in disciplinary action.

10. SPECIFIC RULES FOR ELECTRONIC COMMUNICATION

- 10.1. Employees must not display, transmit, access, store, or create inappropriate, offensive, or unlawful material.
- 10.2. Employees must not engage in online gambling, unauthorized games, chain letters, or use non-approved chat programs or email accounts.
- 10.3. Unauthorized access to software, documents, data, or recordings, including plagiarism, is prohibited.
- 10.4. Employees may not use another person's password or attempt to access another's work without authorisation.
- 10.5. Employees must avoid damaging hardware, software, or computer configurations, including malicious activity such as spreading viruses.

10.6. Email Use

- 10.6.1. Emails must be concise, relevant, and sent only to intended recipients.
- 10.6.2. Confidentiality must be maintained; sensitive information must not be shared inappropriately.
- 10.6.3. Employees should not send abusive, discriminatory, or offensive messages.
- 10.6.4. Deleting emails does not eliminate their retrievability; all emails may be subject to legal disclosure.
- 10.6.5. Private or internal communications should not be shared externally without explicit permission.

11. SOCIAL MEDIA AND DIGITAL MESSAGING

- 11.1. Social media must be used responsibly and in a manner that does not negatively impact the School or its stakeholders.
- 11.2. Employees authorized to speak on behalf of the School must clearly indicate such authority; others must clarify that their views are personal.

- 11.3. Confidential information, learner data, or any inappropriate content must never be shared via social media.
- 11.4. School-related chat groups must not be created without prior approval. Participants must have the opportunity to consent.
- 11.5. Personal social media conduct must not compromise the School's reputation or interests.

12. ASSESSMENT RECORDS, SECURITY, STORAGE, AND REPORTING

- 12.1. Assessment Records: All learner assessment records, including examination papers and progression schedules, are kept securely in physical and digital formats.
- 12.2. Physical Records: Final examination papers are stored in a locked strongroom. Learner profiles and hard-copy reports are kept under lock and key within a secure area.
- 12.3. Digital Records: Attendance, misconduct, and assessment data are captured and managed via the Engage platform (formerly SASAMS). Daily backups and firewall protections are implemented to ensure data security.
- 12.4. Teacher Records: Teachers maintain individual files for their own marks and assessments. The Head of Academics monitors master subject planning files in the staff workroom.
- 12.5. Management Access: Digital records are confidential and accessible only to authorized management staff (Principal, School Secretary, Heads of Departments).
- 12.6. Parental Information: Staff may access parent contact details solely for official communication; editing or sharing such data without authorization is prohibited.
- 12.7. Reports: Learner results are printed centrally and provided to parents; copies are also kept with the Principal and Head of Academics.

13. LEARNER PROFILES

- 13.1. Learner progression schedules and assessment reports are part of the learner's educational profile.
- 13.2. Both digital and physical records are secured, with access strictly limited to authorized personnel.

13.3. Unauthorized disclosure of learner information is strictly prohibited and may result in disciplinary or legal action.

14. COMPLIANCE AND DISCIPLINARY MEASURES

14.1. Any violation of this policy, including misuse of electronic equipment, social media, or mishandling of learner data, will result in disciplinary action.

14.2. Employees are responsible for all activity conducted under their login credentials.

14.3. The network administrator may monitor, maintain, and delete files or accounts as required to ensure compliance with this policy.

14.4. Staff must follow all instructions provided by the network administrator or management regarding ICT use.

15. ACKNOWLEDGMENT

15.1. All employees are required to acknowledge that they have read, understood, and agree to comply with this policy. Breaches may result in disciplinary procedures, up to and including termination of employment.

POLICY TRACKING AND REVIEW RECORD

Policy No. : TBA014
Policy Title : School Data Management Policy
Version Number : V1.0
First Draft Completion Date : 12 November 2025
Approval Date : 12 November 2025
Ratification Date : 13 November 2025
Next Review Due : 12 November 2027