KING WILLIAM'S COLLEGE

King William's College

Cyber Security Policy (with respect to public examinations)

Last reviewed 11/26

Next Review 11/27

Karen Brew (Examinations Officer)

Jo Busuttil (IB Co-Ordinator)

Stuart Corrie (Deputy Head)

Simon Dale-Beeton (Head of IT & Data Management)

1. Introduction

King William's College is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK and Isle of Man legislation, including the Data Protection Act 2018 (both UK and Isle of Man), UK GDPR, Isle of Man GDPR and LED Implementing Regulations 2018, and the latest Keeping Children Safe in Education guidance.

2. Scope

This policy applies to all staff, pupils, governors, and any third parties who have access to King William's College IT systems and data.

3. Roles and Responsibilities

Role	**Responsibilities**
Head of Centre	Damian Henderson (Principal) *Overall responsibility for policy implementation and cyber security strategy.*
IT Manager/Team	Simon Dale-Beeton (Head of IT & Data Management) *Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	Moira Mackie (Chief Operating Officer) *Ensure compliance with data protection law, advise on data handling, and oversee data breaches.*
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Pupils/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

King William's College implements the following security measures, scaled to our size and needs:

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g., Office 365, FireFly).
- Prompt removal of access for leavers.

5. User Account Management

King William's College has procedures in place to maintain the security of user accounts by:

- providing training for authorised staff on the importance of creating strong unique passwords and keeping all account details secret;
- providing training for staff on awareness of all types of social engineering/ phishing attempts;
- enabling additional security settings wherever possible;
- updating any passwords that may have been exposed;
- setting up secure account recovery options;
- reviewing and managing connected applications;
- monitoring accounts and regularly reviewing account access, including removing access when no longer required;
- Access control and permissions are based on job roles and reviewed regularly.
- Giving access to a device which complies with awarding bodies' multi-factor authentication (MFA)
- requireme nts.
- Ensuring that the Exams Office and access obtained by mobile device(s) and laptops outside of network is made via MiFi/mobile 4G router.
- Exam and results information provided via above route if required.
- Results may be downloaded for pupils to receive.
- ensuring that examination candidates' work is backed-up on two separate devices, including two off-site back-ups

6. Staff Training and Awareness

- All staff with access to the school network must complete annual cyber security training and annual refresher training.
  - Phishing awareness and social engineering defence training.
  - Initial Training:
    - https://www.ncsc.gov.uk/section/education-skills/cyber-security-Centres#section_17.
- Records of cyber training must be retained for all staff and be available for inspection.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to Simon Dale-Beeton by emailing: support@kwc.im. This will then be investigated by a member of the IT Team who will assess the impact of a failure or attack and mitigate any possible damage. King William's College has security arrangements in place to protect candidates' work in the event of IT system corruption and cyber-attack.
- Communication plan for stakeholders – The Chief Operating Officer will inform the school's insurer, and the Head of IT will notify the security specialist supplier to assess the potential impact of an incident. In the event of a successful cyber-attack, the risk will be assessed. Where appropriate, the event will be reported to the ICO, local law enforcement, and IOM OCSIA.
- The Examinations Officer or Head of Centre will report any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body. Special Consideration may be applied for in the event of a serious disruption. Exam boards will be contacted to request information required for results to ensure students can still receive them via Awarding bodies secure sites.
- A review to identify lessons learned and update procedures will take place if necessary.

8. Compliance and Auditing

- An annual review and updating of this policy will be conducted by the Deputy Head.
- Regular internal termly audits which are reported to a governor's committee.

9. Policy Review

This policy will be reviewed annually by the Head of IT and Data Management, Deputy Head, Examinations Officer and IB Coordinator and updated as necessary to reflect changes in technology, threats, and best practices.