Weald of Kent Grammar School

Cyber Security Policy (Centre-wide and Exams)

This policy is reviewed annually to ensure compliance with current regulations.

Key staff involved in the policy

Role	Name(s)
Trustee(s)	Quality of Education Committee
Head of Centre	Mr R Booth
Senior Leader(s) i/c exams	Ms A Beasley Mr K MacSporran
Exams Officer	Mrs S Dyos
IT Manager	Mr A Rose

Purpose of the policy

At Weald of Kent Grammar School, the confidentiality, integrity, and availability of our information assets, IT systems, and the personal data of students, staff, and stakeholders are of paramount importance.

This policy establishes our comprehensive cyber security framework, delineates the duties and accountabilities of all relevant parties, and ensures strict adherence to JCQ regulations, the Data Protection Act 2018, the UK General Data Protection Regulation, and the statutory guidance detailed in *Keeping Children Safe in Education*.

This Cyber Security Policy details the measures taken at Weald of Kent Grammar School to mitigate the risk of cyber threats under the following sections:

1. Roles and responsibilities
2. Complying with JCQ regulations
3. Cyber security best practice
4. Account management best practice
5. Training

The senior leadership team recognises the need for staff involved in the management, administration and conducting of examinations to play a critical role in maintaining and improving cyber security at Weald of Kent Grammar School. This includes ensuring that all members of centre staff who access awarding bodies' online systems undertake annual cyber security training.

In addition to adhering to industry best practices, the following areas are addressed in this policy to ensure that members of the exams team protect their individual digital assets:

- Cyber Security Awareness and Training
- Device Security and Asset Register
- Creating strong, unique passwords
- Keeping all account details secret
- 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
- Staying alert for all types of social engineering/phishing attempts
- Monitoring accounts and reviewing account access regularly

Scope

This policy applies to all staff who have access to Weald of Kent's IT systems and data, with particular focus placed upon those members of staff who are involved in the management, administration and conducting of examinations and assessments.

Review

A designated member of the Senior Leadership Team will carry out annual evaluation of this policy, incorporating updates as required to remain abreast of new technologies, threat developments, and industry best practices.

Upon completion of the review and any revisions, the policy will receive formal approval from Trustees.

1. Roles and responsibilities

Trustees

- To oversee and review cyber security arrangements and policy compliance

Head of centre/Senior leadership team

- To provide overall responsibility for policy implementation and cyber security strategy
- To ensure that an up-to-date device security and asset register is maintained which details all computers, devices, and user accounts used for examinations and assessment administration.

This ensures that all technology used is regularly reviewed, patched, and secured, thus reducing the risk of overlooked vulnerabilities being exploited

- To ensure that all devices are secured with up-to-date anti-malware and software updates
- To ensure that members of the exams team, supported/led by the IT team, adhere to best practice(s) in relation to:
    - the management of individual/personal data/accounts
    - centre wide cyber security including:
        - Establishing a robust password policy
        - Enabling multi-factor authentication (MFA)
        - Keeping software and systems up to date
        - Implementing network security measures
        - Conducting regular data backups
        - Educating employees on security awareness
        - Developing and testing an incident response plan
        - Regularly assessing and auditing security controls
        - Managing and reporting a cyber-attack which impacts any learner data, assessment records or learner work

IT Manager/Team

- To implement technical controls, monitor systems, respond to incidents, manage access and updates

Data Protection Officer

- To ensure compliance with data protection law, advise on data handling, and oversee data breaches

All staff

- To follow this policy, complete annual training, report incidents or concerns promptly within the centre

Exams Officer/Exams Assistant

- To ensure that they follow best practice in relation to the management of individual/personal data/accounts
- To provide evidence of an awareness of best practice in relation to cyber security as defined by JCQ regulations/guidance, including the completion of certificated, annual, up-to-date cyber security awareness training
- To undertake training on:
    - the importance of creating strong, unique passwords
    - keeping all account details secret
    - enabling additional security settings wherever possible
    - updating any passwords which may have been exposed
    - setting up/an awareness of secure account recovery options
    - reviewing and managing connected applications
    - awareness of all types of social engineering/phishing attempts
    - reviewing and monitoring account access on a regular basis

Invigilators

- To provide evidence of an awareness of best practice in relation to cyber security as defined by JCQ regulations/guidance, including the completion of certificated, annual, up-to-date cyber security awareness training
- To undertake training on:
    - updating any passwords which may have been exposed
    - awareness of all types of social engineering/phishing attempts
    - reviewing and monitoring account access on a regular basis

Students/users

- To follow this policy and all guidance given through our online safety curriculum delivered through PSHE and Computer Science lessons, report incidents or concerns promptly within the centre.

2. Complying with JCQ regulations

The head of centre/senior leadership team at Weald of Kent Grammar School ensure that there are procedures in place to maintain the security of user accounts in line with JCQ regulations (sections 3.20 and 3.21 of the *General Regulations for Approved Centres* document) by:

- Developing and maintaining this cyber security policy
- Ensuring that all members of centre staff who access awarding bodies' online systems undertake annual, certificated cyber security training which includes:
    - the importance of creating strong, unique passwords
    - keeping all account details strictly confidential
    - the critical role of Multi-Factor Authentication (MFA) in protecting against unauthorised access
    - how to properly set up and use MFA for both centre and awarding bodies' systems
    - an awareness of all types of social engineering/phishing attempts
    - the importance of staff quickly reporting suspicious activity, events and incidents
- Downloading and retaining certificates of completed staff cyber training on file
- Implementing and enforcing robust security measures, including:
    - mandatory Multi-Factor Authentication (MFA) for all accounts and systems containing exam-related information, including those that interface between awarding body and centre systems, to enhance security and protect sensitive data
    - regularly reviewing and updating security settings to align with current best practices
- 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
- Ensuring authorised members of staff securely access awarding bodies' online systems in line with awarding body regulations regarding cyber security and the JCQ document *Guidance for centres on cyber security* (www.jcq.org.uk/exams-office/general-regulations), and that where necessary, they have access to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements
- Reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body

3. Cyber security best practice

The IT Manager at Weald of Kent Grammar School ensures that:

- Security measures are in place including:
    - 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)
    - Prompt removal of access for leavers
- They and all staff involved in the management, administration and conducting of examinations/assessments stay informed about the latest security threats and trends in account security.

- Staff within the exams team are educated on how to identify phishing attempts, use secure devices and how to protect systems and data by online training delivered through The National College.

Best practice, advice and guidance from our internal IT policies and JCQ requirements is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.

By adopting industry standard cyber security best practices, the IT Manager is significantly reducing the risk of cyber-attacks and protecting valuable data and assets within the centre.

If a cyber-attack which impacts any learner data, assessment records or learner work is experienced, the senior leadership team/exams officer will contact the relevant awarding body/bodies immediately for advice and support.

4. Account management best practice

Creating strong unique passwords

- Exams office staff are informed that password length is a more valuable defence than complexity and instructed to use a password creation approach such as three random words to generate suitably secure passwords
- Exams office staff will not use easily guessable information such as birthdays, singular names or common words for a password
- For every account, users are instructed to use a strong unique password and that the same password is not used across any other account(s)
- Passwords at Weald of Kent Grammar School are to be a minimum of 15 characters consisting of at least one lower case, one upper case and a number

Keeping all account details secret

- Exams office staff are instructed never to share login/password details or additional factor/authentication codes with anyone else
- Staff who require access to a system will be given their own, unique user account by the IT Team and never share an account assigned for their use with anyone else.

Enabling additional security settings wherever possible

- All staff will follow awarding body two-factor verification (2FA) or multi-factor authentication (MFA) wherever available/requested. Staff are made aware of the purpose of 2FA /MFA, which includes:
  - adding a layer of account security when a school device is used outside of the school environment
  - helps to protect users if the extra steps/factors are protected

Updating any passwords that may have been exposed

- If it is believed that a password may have been exposed/become known to others, staff will inform their senior leader/line manager or any member of the IT Team, immediately
- Any exposed passwords will be changed as soon as possible, and the new passwords should not be shared with anyone else
- Staff are instructed to use strong unique passwords (e.g. three random words) when changing passwords and that old passwords should not be reused nor should cycling through a small set of passwords across multiple accounts be used

Setting up secure account recovery options

- Account recovery is centrally managed by the IT Team. The centre does not permit self-service password reset for staff accounts.
- Staff who require password resets must contact the IT Helpdesk or attend in person. Password resets are not completed solely via email correspondence.
- The IT Team verify the identity of the staff member directly (in person or via verbal confirmation) before issuing a temporary password. Temporary passwords must be changed at first login.

Reviewing and managing connected applications

- The management of connected applications is overseen by the IT Team. Staff within the exams team do not have local administrative rights to install software or browser extensions.
- Only approved and centrally managed applications may be used on centre devices.
- Exams staff are instructed not to grant permissions to unknown third-party services and to report any unexpected access requests or suspicious prompts to the IT Helpdesk.
- Devices are managed centrally, and application installation is restricted to trusted and approved sources.
- Browser-based password storage is not permitted for exams-related accounts unless managed via an approved secure password manager.

Staying alert for all types of social engineering/phishing attempts

- The centre provides regular cyber security awareness guidance to staff, including the identification of phishing and social engineering attempts.
- Exams staff are instructed never to share passwords, multi-factor authentication (MFA) codes, or approve login requests that they did not initiate.
- Any unsolicited or unexpected emails, messages or phone calls requesting credentials or confidential information are treated with caution. Staff are advised not to click links or download attachments from unknown sources.
- Where communications purport to be from awarding bodies or related organisations, authenticity is verified using official contact details obtained from trusted sources.
- Suspicious emails or suspected phishing attempts are reported to the IT Team immediately for investigation. Where appropriate, incidents referencing awarding bodies are reported to the relevant organisation

Monitoring accounts and reviewing account access

- Staff accounts are centrally managed by the IT Team. Access to systems, including awarding body platforms, is granted based on job role and the principle of least privilege.
- Account permissions are reviewed periodically and amended where roles or responsibilities change.
- User accounts are promptly disabled when a member of staff leaves the centre or no longer requires access.
- The IT Team monitors account activity through centrally managed security tools. Any suspicious or unusual activity is investigated and, where appropriate, reported to the relevant awarding body.
- Exams staff are required to notify the IT Team of any staffing or role changes that may affect access requirements.

5. Training

The head of centre/senior leadership team ensure that there are procedures in place to maintain the security of user accounts by ensuring that all staff who have responsibility for the administration or delivery of examinations complete annual cyber security training and annual refresher training ~~and~~ practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.

Records of cyber training are retained for all staff and are available for inspection

- Certificate for Cyber Security provided by The National College
- Evidence certificate gained at end of course and quiz. Results held by Weald HR Team
- Completed annually