CYBER SECURITY POLICY (Centre-wide & Exams)

2025/26

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	

Key staff involved in the policy

Role	Name(s)
Governor(s)	
Head of centre	Clare Batson
Senior leader(s) i/c exams	Jonny Galbraith
Exams officer	Sarah Adamson
Other staff	Alan Dowsing

Purpose of the policy

At Parklands High 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 Parklands High 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 Parklands High 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
- 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 Parklands High School'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 Mr Jonny Galbraith and Mrs Clare Batson

1. Roles and responsibilities

Governors

- 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
        - 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/Invigilators

- 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

Students

- To follow this policy and report incidents or concerns promptly within the centre

2. Complying with JCQ regulations

The head of centre/senior leadership team at Parklands High 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 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
- 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)
- 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 head of centre/senior leadership team at Parklands High School ensure 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
    - Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
    - 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.
- Best practice, advice and guidance from The National College training system is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.

National Cyber Security Centre (NCSC) training and guidance is followed at Parklands High School which includes:

- Establishing a robust password policy
- 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

The Exams Office training and guidance is followed at [insert centre name] which includes:

- Good practice in creating strong and unique passwords
- Account security: Keeping account details secret (including sharing passwords, remembering passwords and monitoring account access)
- Additional security settings (including, multi-factor/two-step/two-factor authentication, the security of confidential examination materials)
- Updating expired or exposed passwords
- Account recovery (including recovery options)

- Reviewing and managing connected applications (including reviewing and removing access, using a third-party or a cloud service, granting permissions, saving passwords, saving details on local web browsers, using a shared browser)
- Social engineering/phishing attempts (including suspicious emails and phone calls, sharing information, QR codes, phishing attempts, recovery plan)
- Monitoring and reviewing access (including suspicious, unusual or unauthorised activity, departing staff, levels of access, reviewing user accounts)

Exam specific guidance is also provided on each of the areas listed above

By adopting industry standard cyber security best practices, the head of centre/senior leadership team are 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
- 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

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 with practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.