



Cyber Security Policy (Exams)

Southend High School for Girls

Cyber Policy

Centre name	Southend High School for Girls
Centre number	16607
Current policy approved by	Governors/SLT
Current policy reviewed by	Lesley McFee; Helen Riebold; David Morris
Date of review	01/12/2025
Date of next review	01/12/2026

Key staff involved in the policy

Role	Name
Head of centre	Jason Carey
Senior leader(s)	Jason Carey; Helen Riebold; Penny Bowman; Anna Leman; Isobel Boyson, Rebecca McMahon and Robert Prior
Exams officer	Lesley McFee
Other staff (if applicable)	David Morris (IT Manager) Invigilators (appendix 1) Emma King (Data Protection Officer)

This policy is reviewed and updated annually to ensure that conflicts of interest at Southend High School for Girls are managed in accordance with current examination requirements and regulations. Reference in the policy to **GR** relates to relevant sections of the current JCQ document **General Regulations for Approved Centres**.

SHSG maintain an additional **whole school Cyber Security Policy** approved by Governors.

Purpose of the policy

At Southend High School for Girls, 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 Southend High School for Girls 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 Southend High School for Girls. 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 Southend High School for Girls' 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.

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
 - 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 ensure that they follow best practice in relation to the management of individual/personal data/accounts.

Students/users

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

2. Complying with JCQ regulations

The head of centre/senior leadership team at Southend High School for Girls 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 head of centre/senior leadership team at Southend High School for Girls 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
 - Multi-factor authentication (MFA) for critical systems and remote access
 - 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 by completing the yearly cyber training with the National College.

Best practice, advice and guidance from David Morris, IT Manager 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 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

All centre users are reminded in their annual online safety training of the importance of password protection.

Keeping all account details secret

All centre users are reminded in their annual online safety training of the importance of never sharing their login/password, or additional factor/authentication codes with anyone.

Enabling additional security settings wherever possible

Where is it available, centre staff will use any secure account recovery options available, which may include alternate emails accounts or phone numbers protected by 2SV/2FA/MFA security measures.

Updating any passwords that may have been exposed

All centre users are reminded in their annual online safety training of the importance of password protection. Should a centre user believe their password has been exposed/known to anyone, they will report to IT and a senior leader and change their password.

Setting up secure account recovery options

Where is it available, centre staff will use any secure account recovery options available, which may include alternate emails accounts or phone numbers protected by 2SV/2FA/MFA security measures.

Reviewing and managing connected applications

Should a member of staff receive unsolicited or unexpected emails, instant messages or a phone call, they would contact the IT team for investigation.

Staying alert for all types of social engineering/phishing attempts

All centre staff complete annual online safety course via National College.

Should a member of staff receive unsolicited or unexpected emails, instant messages or a phone call, they would contact the IT team for investigation.

Monitoring accounts and reviewing account access

The HR department provide a list of leavers to the Exams Officer on a termly basis. The Exams Officer will review the users of the Exam Boards software to ensure only active staff have online access and the correct level of 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.

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

- *Annual Online training via National College*

6. Appendix 1: List of invigilators

Armelle	Binns
Asna	Butt-Alam
Brenda	Marron
Claire	Rayner
Denise	Robertson
Gail	McAllister
Jacqueline	Raja
Joanne	Cobbold-Clark
Joanne	Jerman
John	Boswell
Lisa	Hart
Moir	Al-Shaar
Nathalie	Quigley
Pamela	Smith
Sarah	Brown
Sofia	Pileci
Stephanie	Wheeler
Steven	Raybould
Tina	Boswell
Tracey	Cooper
Katie	Carter-Leay
Dave	Griffin
Karen	Middleton
Claire	Sharp
Kai	Lee
Kayla	Situ
Cherylyn	Fry
Deborah	Robertson
Fiona	Jones
Beverley	Earls
Jacqueline	Balmer
Caroline	Gunn