Cyber Contingency Plan (examinations)

Centre name	The Roundhill Academy
Centre number	25327
Date policy reviewed	31 October 2026
Policy approved by	Natalie Teece
Policy reviewed by	Julia Rann
Date of next review	30 September 2027

Key staff involved in the policy

Role	Names
Head of Centre	Natalie Teece
SLT Member with responsibility for Exams	Julia Rann
Examinations Manager	Tania Taylor
IT Development Manager	Dan Perkins

This policy is reviewed annually to ensure compliance with current regulations and reflects centre practice.

To be read in conjunction with

- BEP IT Policy

Purpose of the policy

At The Roundhill Academy, 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 policy details the measures taken at The Roundhill Academy 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 The Roundhill Academy. 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 The Roundhill Academy'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 the key staff involved in the creation of this policy

Introduction

This plan is to be enacted when requested by the Cyber response team in the event of a cyber incident occurring that may affect an examination.

Any serious interruption to IT at the following critical stages may cause a problem to the exams process:

- Exam entries to be submitted to exam boards (start of October and during January and February)
- BTEC registrations to be submitted (start of November)
- Access Arrangement to be applied for by the SENCO throughout the academic year
- Exam entry amendments / withdrawals to be submitted (February until end of June)
- Internal assessments (NEA) marks to be uploaded by teachers onto exam board secure websites during April and May
- Exam rooms and seating exercise to produce exam timetables for students October and March onwards
- The weeks prior to exams start of January and all of May and June
- On the day of the exams (November, January and May and June)
- Special Consideration applications to be submitted to exam boards (November, January and May-July)
- Results times (January, March and mid to end of August)
- Post Results Services applications to be submitted to exam boards (January, March and August and September)

These are the critical systems for access to be maintained (throughout the academic year):

- Arbor
- A2C
- Printing
- Email
- Awarding body websites (including their various secure websites)

Below are the contact details for the Examination Boards:

Exam Board	Contact
AQA	AQA Customer Services team / Exams Officers enquiries: Email: eos@aqa.org.uk Tel: 0800 197 7162 Website: https://www.aqa.org.uk Opening hours: 08:00–17:00 Mon to Fri
OCR	OCR Customer Support Centre: Email: support@ocr.org.uk Tel: 01223 553998 Website: https://ocr.org.uk Opening hours: Mon to Fri 08:00–17:00 (closed Tues and Thurs - 12:00–13:00 for staff training).

Pearson	Pearson Helpdesk / Support Centre: Email: examsofficers@pearson.com Tel: 0344 463 2535 Website: https://qualifications.pearson.com/en/home.html Opening hours: 08:00–17:00 Mon to Fri.
WJEC /Eduqas	WJEC Helpdesk / Support Centre: Email: (WJEC: info@wjec.co.uk) - (Eduqas: info@eduqas.co.uk) Tel: (WJEC: 029 2027 5000) - (Eduqas: 029 2027 5465) Websites (WJEC): https://www.wjec.co.uk/home/about-us/useful-contacts/ (Eduqas): https://www.eduqas.co.uk/home/about-us/useful-contacts/ Opening hours: 08:00–17:00 Mon to Fri.

Upon being made aware of a possible cyber attack, the Examinations Manager should inform the awarding body(ies) and ensure, whenever possible, that the exams can go ahead.

Exam entries, BTEC Registrations, Entry Amendments/Withdrawals and Results:

Arbor is required at all times.

Use of A2C software is also required. A2C will be installed on more than one member of staff's PC (Exams Manager and Julia Rann) and on one of the contingency "Clean" laptops.

Prior to exams:

Access arrangements to be applied for by the SENDCO. If the internet is not available, where possible, this exercise can be carried out at the sister secondary school (Wreake Valley Academy).

Teachers need to submit Internal Assessment Marks to exam boards. If the internet is not available, where possible, this procedure can be carried out at Wreake Valley Academy.

Student lists are downloaded from Arbor for exams. If the internet is not available, then the clean laptop and 4G dongle can be used.

Exam timetables are printed out and given to students. Printing will be available either on a standalone USB printer or, where possible, at Wreake Valley Academy.

Reminders are emailed to students and parents. If email is down, these can be printed and handed out.

On the day of the exam:

Some students require laptops, these are offline devices so will be unaffected by any Cyber incident.

On screen exams may need to be moved to Wreake Academy, or The Cedars Academy or cancelled. A decision will need to be made by Head of Centre and IT Manager, depending on the exact nature of the cyber incident. Awarding body(ies) will need to be informed by the Examinations Manager.

Listening exam audio files for Modern Foreign Language and Music need to be downloaded on the morning of the exam. This can be done on any computer with internet access. The files can then be distributed to run on the exam laptops using a clean memory stick. In an event of a total internet

unavailability, CDs / DVDs (where provided by exam boards) can be used on standalone laptops. Where these are not available, Examinations Manager will contact awarding body

Printing of exams on coloured paper can either be done on a standalone USB printer or, where possible, at Wreake Valley Academy. Eastfield Primary School has agreed to allowing the use of their facilities in the event of both secondary schools being affected.

Post exams:

If the internet is not available, where possible, the procedures listed below can be carried out at Wreake Valley Academy.

- Special Consideration applications
- Downloading Results and printing
- Post Results Services

In case of internet failure at both secondary schools the Headteacher at Eastfield Primary School, a local school in the BEP Trust has agreed to support with internet access. In the event of a Trust-wide issue The Cedars Academy has agreed to support with internet access.

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 manager

- 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 annual, up-to-date cyber security awareness training

To undertake training which must include:

- the importance of creating strong, unique passwords
- keeping all account details secret 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 any suspicious activity, events, incidents and encouraging a safe and supportive reporting culture

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 The Roundhill Academy must ensure that there are procedures in place to maintain the security of user accounts in line with JCQ regulations (section 3. of the *General Regulations for Approved Centres* document) by:

- Developing and maintaining this comprehensive cyber security policy
- Ensuring that all members of centre staff who access awarding bodies' online systems undertake annual cyber security training
- Holding a record of completed staff cyber security training on file for inspection (This record could take the form of a certificate, a paper checklist, a spreadsheet-based checklist or a Learning Management System (LMS) report)
- Implementing and enforcing robust security measures, including:

- where available, MFA must be used 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 (Where MFA is not available on the centre's systems, an equivalent multi-layered security approach must be in place. For example, strong log-in controls, access and monitoring controls and secure storage so that exam-related data is protected in line with cyber security best practice.)
- regularly reviewing and updating security settings to align with current best practices
- 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' 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 following are some essential guidelines for managing systems and user accounts securely. This guidance should be followed for all awarding body user/email accounts that are used to provide or manage access to awarding body systems, information or data. By following these best practices, centres and centre staff can significantly reduce the risk of unauthorised access and protect sensitive information and other valuable assets.

The head of centre/senior leadership team at The Roundhill Academy 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 online training and INSET

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

Cyber Security Awareness and Training

The Roundhill Academy ensures that:

- all staff who have responsibility for the administration or delivery of examinations receive annual, up-to-date cyber security awareness training, with practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.

  Attackers often target school or college staff to gain access to assessment systems by tricking them through deceptive messages or phone calls.

4. Account management best practice

Creating strong unique passwords

- Password governance follows National Cyber Security Centre guidance
- 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)

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 request their own user account and never share an account assigned for their use with anyone else. Staff are reminded that anything done with an account assigned to someone will be attributed to that person in the first instance

Enabling additional security settings wherever possible

- All staff will follow awarding body two-step verification (2SV)/two-factor verification (2FA) or multi-factor authentication (MFA) wherever available/requested. Staff are made aware of the purpose of 2SV/2FA /MFA, which includes:
    - adding a layer of account security
    - 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 immediately
- Any exposed passwords will be changed as soon as possible, and the new passwords should not be shared with anyone
- 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

- Staff are instructed to follow centre account recovery options which may include alternate email accounts or phone numbers protected by 2SV/2FA/MFA security measures

Reviewing and managing connected applications

- Staff within the exams team will regularly review and remove access for third-party applications or services that no longer require access to accounts
- Staff will be informed that access should only be provided to trusted services
- Staff will be asked to be particularly cautious when interacting with content and services (e.g. quizzes, prize draws, surveys etc.)
- Staff will only grant permissions to required applications or the necessary access to allow them to function
- Staff will only download and install applications with established reputations from trusted sources
- Staff will not save passwords to local web browsers unless a secure password manager extension is used in a browser that requires unlocking (e.g. with another password) before the saved account details can be retrieved, however care will be taken to ensure that this is locked/signed out of after use

Staying alert for all types of social engineering/phishing attempts

- received asking for account credentials or personal or confidential information. Passwords and 2FA/MFA authentication codes should not be given out to anyone

- Staff are instructed that they should have a wariness of anyone or anything that seems to want to gain their trust, rush them into doing something or that just seems off, they should hang up/not reply and not click on links or take any action and check with a trusted party via a secure channel (i.e. call awarding body customer services via a known support number)
- Staff will never approve or authenticate a login request that they did not initiate
- Staff will not share codes/approve logins. Requests to share codes/approve logins should be treated with a high degree of suspicion
- Staff will not click on suspicious links, download attachments or scan QR codes from unknown sources
- The centre will provide exams team staff with a secure QR code scanner with a good reputation to help gauge whether a QR code is suspicious or malicious
- Staff will verify the authenticity of any communication by contacting the organisation directly through official known channels
- Staff will report any phishing attempts which reference awarding bodies/their systems to the awarding body concerned immediately

Monitoring accounts and reviewing account access

- Centre staff accounts will be routinely reviewed for any suspicious, unusual or unauthorised activity
- If any suspicious, unusual or potentially unauthorised activity on awarding body systems is observed this will be immediately reported to the relevant awarding body, particularly if it is believed that user account security may have been compromised
- Access control and permissions are based on job roles and reviewed regularly
- Levels of access for all exams team staff are reviewed regularly to ensure accounts have the minimum level of access required for their current role
- Accounts are promptly disabled when users leave
- Account activity is monitored and audited

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 with practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.
- Records of completed cyber security training are retained for all staff and are available for inspection – this is annual face to face training on INSET day and online BEP training.

Device Security and Asset Register

The Roundhill Academy:

- Maintains an up-to-date register of all computers, devices, and user accounts used for examinations and assessment administration.

- All devices are secured with up-to-date anti-malware and software updates. Keeping a full register ensures that all technology used is regularly reviewed, patched, and secured, reducing the risk of overlooked vulnerabilities being exploited.

The Roundhill Academy uses Microsoft Intune Office 365 for this purpose.

Keep all account details secret

Staff at The Roundhill Academy must:

- Never share login/password details or additional factor/authentication codes with anyone else.

  Attackers will often try to trick people into sharing those details with them by pretending to be from their awarding body, a technical support team or other organisation.

- Request their own access to a system and never share an account assigned for their use with anyone else.

  Remember that anything done with an account assigned to someone will be attributed to that person in the first instance.

Update any passwords that may have been exposed

- If it is believed passwords may have been exposed/become known to others, they should be changed as soon as possible. The new passwords should not be shared with anyone.

- When changing passwords, strong unique passwords (e.g. three random words) should always be used. Old passwords should not be reused nor should cycling through a small set of passwords across multiple accounts be used.

  When passwords are reused, or follow a discernible pattern, attackers have tools that will help them to identify such password reuse/cycling patterns.

Set up secure account recovery options

- Updated account recovery options, such as alternate email accounts or phone numbers, should be set up or maintained to facilitate access to accounts in case of a lockout or compromise.

  Attackers will try to use account recovery options (e.g. another email account specified as the recovery account) to take over an account, so wherever possible 2SV/2FA/MFA security should be enabled on all such accounts to ensure they remain secure from hackers.

Review and manage connected applications

The Roundhill Academy will:

- Ensure all devices and networks used for exams have appropriate web filtering (to block access to malicious websites) and monitoring (to alert you to unusual or unauthorised activity).

Filtering and monitoring help prevent staff from reaching unsafe websites and quickly alert you if attackers attempt to compromise systems or assessment data.

The Roundhill Academy uses Smoothwall and Senso Cloud for this purpose

- Regularly review and remove access for third-party applications or services that no longer require access to accounts.

  Attackers can breach services that users have been given access to and then use that access to attempt to access the user's accounts. Access should only be provided to trusted services. Centre staff should be particularly cautious when interacting with content and services (e.g. quizzes, prize draws, surveys etc.) on social media platforms as these are often used by attackers to access user information.

- Before using any third-party or cloud service for exams or assessments, check that the supplier meets recognised cyber security standards and put a data processing agreement in place.

  Attackers may target suppliers or cloud platforms, or data could be mishandled. Carrying out these checks and having a formal agreement helps keep sensitive assessment information secure and ensures your centre remains legally compliant.

- Be cautious when granting permissions to applications and grant only the necessary access required for them to function.

  This is particularly relevant where apps ask for permissions that don't seem to make sense given the nature of the app. For example, a Word Search app that wants access to a user's contacts and be able to send SMS messages should be regarded with suspicion. Only download and install applications with established reputations from trusted sources.

- Passwords should not be saved to local web browsers. This is particularly important where there is shared access to a device or web browser. An exception to this is where a secure password manager extension is used in a browser that requires unlocking (e.g. with another password) before the saved account details can be retrieved, however care should be taken to ensure that this is locked/signed out of after use.

- Saving account details (usernames/passwords) on local web browsers that anyone using that browser can then access weakens account security. Enabling additional security controls on accounts such as 2SV/2FV/MFA or using a secure password manager can prevent others from accessing accounts in such circumstances.

- When using a shared browser, the browser history and cache should be cleared out after use. The use of private browsing functions to reduce the usage trail left on any such browser should also be considered.

Stay alert for all types of social engineering/phishing attempts

- Care should be taken if unsolicited or unexpected emails, instant messages, or phone calls are received asking for account credentials or personal or confidential information. Passwords and 2FA/MFA authentication codes should not be given out to anyone.

  Attackers will often try to 'hack the human' first as it's cheaper and quicker for them than a technical attack. Centre staff should develop a healthy wariness of anyone or anything that

seems to want to gain their trust, rush them into doing something or that just seems off. If in doubt, hang up/don't reply and don't click on links or take any action and check with a trusted party via a secure channel (i.e. call awarding body customer services via a known support number).

- Users should never approve or authenticate a login request that they did not initiate.

  Attackers who obtain a username and password will try to get the user to share any 2FA/ MFA code with them or to approve the login request via some other means. They may try to convince the user that they need to confirm their identity and will send a secret code that the user needs to read out to them or ask for approval of a request they send in an authenticator app. In reality they are attempting to login to the account, are triggering the 2FA/MFA challenge and are trying to trick the user into giving them that code or approving access. Requests to share codes/approve logins should not be approved and requests to do so should be treated with a high degree of suspicion.

- Do not click on suspicious links, download attachments or scan QR codes from unknown sources.

  QR codes are easy for attackers to generate and are being increasingly used in phishing attacks. Caution is needed when scanning a QR code and wherever possible a secure QR code scanner with a good reputation should be used to help gauge whether a QR code is suspicious or malicious.

- Verify the authenticity of any communication by contacting the organisation directly through official known channels.

  Be wary of unsolicited inbound phone calls even where the caller's number appears genuine. Attackers will sometimes use number 'spoofing' services that mask their real number and make it look like the call is from a genuine trusted number. If in doubt, hang up and call back via a known trusted number.

- Report any phishing attempts which reference awarding bodies/their systems to the awarding body concerned immediately.

  JCQ and awarding bodies can send out communications to centres where notable attacks are observed, but rely on centres and centre staff to flag notable attacks to them. Any such attempts should be reported to awarding bodies.

- Ensure systems used for assessment administration are included within your centre's disaster recovery and business continuity plans. Test your ability to recover data and restore normal assessment operations at least once each year.

  A tested recovery plan ensures that systems can be maintained or quickly resumed after a cyber incident, protecting candidates and safeguarding results.

Monitor accounts and review account access regularly

- Centre staff accounts should be routinely reviewed for any suspicious, unusual or unauthorised activity.

  If any suspicious, unusual or potentially unauthorised activity on awarding body systems is observed this should be immediately reported to the relevant awarding body, particularly if is believed that user account security may have been compromised.

- Ensure user access is reviewed promptly for staff who have left the centre.

  Leaving ex-employee access in place increases the danger of inappropriate/unlawful access to systems and data.

- Review levels of access regularly to ensure accounts have the minimum level of access required for their current role.

  Over-privileged accounts present an increased risk should an attacker gain access to the centre's systems. It might seem easier to give staff access to everything, but if an attacker gets into a user account, they will also have access to everything!

Guidance from NCSC and DfE

Centres should stay informed about the latest security threats and trends in account security and educate staff on how to identify phishing attempts, secure devices and protect systems and data.

Both the National Cyber Security Centre (NCSC) and the Department for Education (DfE) have published up-to-date guidance, which all centres should follow. This guidance covers the steps schools and colleges need to take to keep assessment and learner data safe, and to reduce the risk of problems caused by cyber attacks.

This guidance covers the steps schools, colleges and other educational establishments need to take to keep assessment and learner data safe, and to reduce the risk of problems caused by cyber attacks.

Key recommendations include:

- 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
- Training staff annually on security awareness
- Having a tested Incident response plan
- Regularly assessing and auditing security controls

  By adopting these industry standard cyber security best practices, centres can significantly reduce the risk of cyber attacks and protect their valuable data and assets.

  If centres experience a cyber attack which impacts any learner data, assessment records or learner work, they should contact their awarding body immediately for advice and support.

Training in the Bradgate Education Partnership

All staff in the trust receive annual training and must complete cyber training on the Bradgate Learning Hub.

Test phishing emails are sent out regularly. Failure to report a phishing email results in staff redoing the training

All staff are aware of how to secure devices with strong passwords and are recommended to use password manager to generate and securely store strong, unique passwords for work accounts.

Data is regularly backed up and stored in the cloud – The Roundhill Academy uses Barracuda.

Access to sensitive information is limited to those staff who require access to it.

Bradgate Education Partnership regularly push out software updates for all staff to complete.

The Exams Manager will complete the Exams Office Cyber training and will have the certificate available for inspection by the JCQ Inspection Service.