Exam Contingency Plan

Lealands High School

Exams Policy –

Contingency Plan

Lealands High School (SFR)

October 2025

Exam Contingency Plan

Contents

INTRODUCTION

Lealands High School policies are designed to support the school ethos, aims and vision. Lealands is a positive learning community which is fully inclusive to ensure equality of opportunity for all.

Our aims are outlined in our Home School Agreement.

Our aims:

Excellence in everything we do	Everyone has responsibility	Respect for all
● Everyone achieves success and makes excellent progress	● To prepare young people for life and a positive future	● Everyone is valued for their contribution
● We all continually improve what we do and work hard	● To ensure that school is a safe place	● All are cared for and supported so that needs are met
● We care about being the best we can be and getting the best out of those around us	● To help and support others to grow and succeed	● We recognise and celebrate the talents, gifts and uniqueness of every individual

In order to achieve these aims students, parents and the school need to work in partnership.

Our vision is to be:

*Everyone **achieves excellence**, demonstrates **respect** for all and takes **responsibility** for their own actions, while helping others to be successful.*

We strive to achieve this vision in all that we do and staff, students, parents, governors, other school stakeholders and partners are all an important part of making this happen.

Purpose of the plan

This plan examines potential risks and issues that could cause disruption to the exams process. By outlining actions/procedures to be invoked in case of disruption it is intended to mitigate the impact these disruptions have on our exam process.

Alongside internal processes, this plan is informed by the *Exam system contingency plan: England, Wales and Northern Ireland*.

This plan is compliant with the JCQ regulation (section 5.3, *General Regulations for Approved Centres*) that the centre has in place a written examination contingency plan which covers all aspects of examination administration. This will allow members of the senior leadership team to act immediately in the event of an emergency or where the head of centre, examinations manager or SENCo is absent at a critical stage of the examination cycle.

National Centre Number Register and other information requirements

The head of centre will also ensure that Lealands High School as a contingency to enable the prompt handling of urgent issues only, responds to the awarding bodies' request for information regarding the contact details of a senior member of staff (which might include a personal mobile number and/or email address). This will ensure that any urgent matters which might adversely affect candidates which arise outside of term time, and which potentially put qualification awards at risk, can be addressed by awarding bodies with the support of that member of staff. Heads of centre should ensure that this member of staff has the necessary authority to mobilise resources to provide this support, which might include resolving issues within the centre itself.

Possible causes of disruption to the exam process

1. **Exam officer extended absence at a critical stage of the examination cycle.**

Criteria for implementation of the plan

Key tasks required in the management and administration of the exam cycle not undertaken including:

Planning

- annual data collection exercise not undertaken to collate information on qualifications and awarding body specifications being delivered
- annual exams plan not produced identifying essential key tasks, key dates and deadlines
- sufficient invigilators not recruited

Entries

- awarding bodies not being informed of early/estimated entries which prompts release of early information required by teaching staff
- candidates not being entered with awarding bodies for external exams/assessment
- awarding body entry deadlines missed or late or other penalty fees being incurred

Pre-exams

- invigilators not trained or updated on changes to instructions for conducting exams
- exam timetabling, rooming allocation; and invigilation schedules not prepared
- candidates not briefed on exam timetables and awarding body information for candidates

- confidential exam/assessment materials and candidates' work not stored under required secure conditions
- internal assessment marks and samples of candidates' work not submitted to awarding bodies/external moderators

Exam time

- exams/assessments not taken under the conditions prescribed by awarding bodies
- required reports/requests not submitted to awarding bodies during exam/assessment periods, for example very late arrival, suspected malpractice, special consideration
- candidates' scripts not dispatched as required for marking to awarding bodies

Results and post-results

- access to examination results affecting the distribution of results to candidates
- the facilitation of the post-results services

Centre actions to mitigate the impact of the disruption

- Acting Exams Officer appointed as soon as possible, ensuring key tasks are understood.
- Exams Officer to ensure essential information is available to the Senior Leadership Team
- Exams Officer to ensure the Exam Cycle, policies and procedures are up to date at all times.

2. SENCo extended absence at a critical stage of the examination cycle.

Criteria for implementation of the plan

Key tasks required in the management and administration of the access arrangements process within the exam cycle not undertaken including:

Planning

- candidates not tested/assessed to identify potential access arrangement requirements
- centre fails to recognise its duties towards disabled candidates as defined under the terms of the Equality Act 2010
- evidence of need and evidence to support normal way of working not collated

Pre-exams

- approval for access arrangements not applied for to the awarding body
- centre-delegated arrangements not put in place
- modified paper requirements not identified in a timely manner to enable ordering to meet external deadline
- staff providing support to access arrangement candidates not allocated and trained

Exam time

- access arrangement candidate support not arranged for exam rooms

Centre actions to mitigate the impact of the disruption

- Assistant SENCo/experienced member of SEN team to understand and implement key tasks.
- Testing and assessments continue to be carried out by SEN team and Qualified Assessor Applications for Access Arrangements to me made in conjunction with the Exams Officer.
- SENCo and Assistant SENCo to be fully conversant and up to date with JCQ Access Arrangements and Reasonable Adjustments.

3. Director of Subject staff extended absence at a critical stage of the examination cycle.

Criteria for implementation of the plan

Key tasks not undertaken including:

Early/estimated entry information not provided to the exams officer on time; resulting in pre-release information not being received

Final entry information not provided to the exams officer on time; resulting in candidates not being entered for exams/assessments or being entered late/late or other penalty fees being charged by awarding bodies

Non-examination assessment tasks not set/issued/taken by candidates as scheduled

Candidates not being informed of centre assessed marks before marks are submitted to the awarding body and therefore not being able to consider appealing internal assessment decisions and requesting a review of the centre's marking

Internal assessment marks and candidates' work not provided to meet awarding body submission deadlines
Centre actions to mitigate the impact of the disruption ► 2nd in department to undertake key tasks ► Candidates being informed of centre assessed marks, forms part of Exams Policy, which all staff are responsible for being familiar with.

4. Invigilators - lack of appropriately trained invigilators or invigilator absence

Criteria for implementation of the plan Failure to recruit and train sufficient invigilators to conduct exams Invigilator shortage on peak exam days Invigilator absence on the day of an exam
Centre actions to mitigate the impact of the disruption ► New and existing Invigilators receive regular training and are familiar with JCQ requirements ► Invigilation allocated in advance with provisions in place for shortages to be filled by additional Invigilators and/or trained school staff. ► Names and contact numbers of pool of Invigilators kept in Exams office

5. Exam rooms - lack of appropriate rooms or main venues unavailable at short notice

Criteria for implementation of the plan Exams officer unable to identify sufficient/appropriate rooms during exams timetable planning Insufficient rooms available on peak exam days Main exam venues unavailable due to an unexpected incident at exam time
Centre actions to mitigate the impact of the disruption ► Exam venues are allocated in advance of exam season to ensure rooms made available.

- Majority of exams are held in the sports area. If a main venue becomes unavailable it will be possible to rearrange venues using seating plans and classroom timetables.
- Exams Officer to ensure that any room changes comply with JCQ regulations

6. Cyber-attack

Criteria for implementation of the plan Where a cyber-attack may compromise any aspect of delivery
Centre actions to mitigate the impact of the disruption School has in place properly configured firewall protection Firewall firmware is kept up to date . Monitoring logs kept and checked

7. Failure of IT systems

Criteria for implementation of the plan *MIS system failure at final entry deadline* MIS system failure during exams preparation MIS system failure at results release time
Centre actions to mitigate the impact of the disruption - Liaise with IT to resolve any issue. - Exams Officer to contact exam boards to identify alternative and/or make entries, receive results via exam board secure websites - Exams Officer to contact exam boards to inform of any on-going situations

8. Emergency evacuation of the exam room (or centre lockdown)

Criteria for implementation of the plan Whole centre evacuation (or lockdown) during exam time due to serious incident resulting in exam candidates being unable to start, proceed with or complete their exams
Centre actions to mitigate the impact of the disruption

- All Invigilators and Exams Officer to ensure emergency evacuation plan is followed, maintaining the integrity of the exam.
- Candidates have designated evacuation area to avoid contact with other students. Invigilators to ensure do not talk to one another.

9. Disruption of teaching time – centre closed for an extended period

Criteria for implementation of the plan
Centre closed or candidates are unable to attend for an extended period during normal teaching or study supported time, interrupting the provision of normal teaching and learning
Centre actions to mitigate the impact of the disruption
► Prioritise teaching venues for students in exam years where possible ► Exams Officer to inform exam boards of situation ► Consider use of alternative venues.

10. Candidates may not be able to take examinations – centre remains open

Criteria for implementation of the plan
Candidates may not be able to attend the examination centre to take examinations as normal
Centre actions to mitigate the impact of the disruption
► Exams Officer to inform exam boards of situation. ► Exams Officer to consider whether application for Special Consideration is required ► Consider use of alternative venues

11. Centre unable to open as normal during the exams period

Criteria for implementation of the plan
Centre unable to open as normal for scheduled examinations
Centre actions to mitigate the impact of the disruption

- The school will be open for examination candidates unless a situation means that it is unsafe for anyone to enter the building.
- Exams Officer to inform exam boards of situation.
- Consider use of alternative venues: The Meads, Leagrave Primary.
- Centre to communicate with parents/carers regarding any change in venues.
- Centre has contingency days in line with JCQ regulations.
- Information to be made available via school's website

12. Disruption in the distribution of examination papers

Criteria for implementation of the plan

Disruption to the distribution of examination papers to the centre in advance of examinations

Centre actions to mitigate the impact of the disruption

- Exams Officer to communicate with awarding organisation(s) to organise alternative delivery of papers.

13. Disruption to the transportation of completed examination scripts

Criteria for implementation of the plan

Delay in normal collection arrangements for completed examination scripts

Centre actions to mitigate the impact of the disruption

- Exams Officer to communicate with awarding organisation(s) to resolve issue.
- Scripts to be stored securely in accordance with JCQ regulations until issue resolved.

14. Assessment evidence is not available to be marked

Criteria for implementation of the plan
Large scale damage to or destruction of completed examination assessment evidence before it can be marked
Centre actions to mitigate the impact of the disruption
► Exams Officer/SLT to communicate with awarding organisation to seek advice and further instructions.

15. Centre unable to distribute results as normal

Criteria for implementation of the plan
Centre is unable to access or manage the distribution of results to candidates, or to facilitate post-results services
Centre actions to mitigate the impact of the disruption
► Exams results to be accessed via awarding body secure websites. ► If unable to distribute results, the centre will communicate with parents/carers with details of alternative arrangements. ► Information to be made available via school's website ► If unable to facilitate post result services, the centre will communicate with the awarding organisation to seek advice.

Cyber Security Policy

Purpose

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions could cause great damage and may jeopardise our school's reputation or threaten our finances.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope
This policy applies to all our staff, governors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Roles and Responsibilities
As managing ICT and e-safety are important aspects of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Policy elements
Confidential data is private and valuable. Common examples are:

- Data of students/parents/carers
- Financial data
- Personal information

All staff are obliged to protect this data. In this policy, we will give our staff instructions on how to avoid security breaches.

Threats
A threat if left unchecked, it could disrupt the day-to-day operations of the school, the delivery of education and ultimately has the potential to compromise local and national security.

Types of Threats
a) Cybercriminals and Cybercrime
Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means. Key tools and methods used by cybercriminals include:

- Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals • Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

b) Hacktivism
Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

c) Insiders
Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

d) Zero-day threats

A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

e) Physical threats
The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

f) Terrorists
Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

g) Espionage
Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.

10 Steps to Cyber Security
At Lealands, we aim to implement the National Cyber Security Centre's advice for keeping our data secure:

Data and information used

- Student and Staff information in our Management Information System (SIMS)
- Child Protection information (CPOMS)
- Communication – emails and messages through gmail and WEDUC
- Curriculum and Teaching materials
- Records of information (meetings, presentations, etc)

Protect personal and school devices
In general, staff should try to only use school-issued devices to access school emails, accounts or folders. When staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected.
- Ensure that the school-installed antivirus software (ESET) is installed on their school owned computer and that they have anti-virus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log into school accounts and systems through secure and private networks only.

We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they will receive instructions for: ● Password management setup

Antivirus / anti-malware software is installed on all school-owned laptops / devices and we advise all staff to have anti-virus software installed on their own devices. .

Staff must follow instructions to protect their devices.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct staff to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a member of staff isn’t sure that an email they received is safe, they can check with Mark Browne the IT support personnel.

See the section in the Acceptable Use of ICT Policy for further details on email etiquette and email security.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays). General guidance on creating a password is to take three random words and to add a number and a special character – eg. DinosaurStarRose14%
- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn’t possible, staff should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Whilst some providers and organisations with whom we work advise (and expect) passwords to be changed regularly, we advise that passwords only be changed if and when they are compromised.

Transfer data securely

Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, staff records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request staff to ask our IT provider

(PEL) for help.

- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Ensure that data is sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility)
- Report scams, privacy breaches and hacking attempts
- Our IT Provider needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we require our staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Provider will investigate promptly, resolve the issue and send a schoolwide alert when necessary.

Our IT Team is responsible for advising staff on how to detect scam emails. We encourage our staff to reach out to them with any questions or concerns.

Additional measures
To reduce the likelihood of security breaches, we also instruct staff to:

- Turn off screens and lock devices when leaving desks.
- Report stolen or damaged equipment as soon as possible to Mbrowne@lealands.luton.sch.uk
- Change all account passwords at once if a device is stolen.
- Report a perceived threat or possible security weakness in school systems. ● Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites.

We also expect staff to comply with our social media and Acceptable Use of

ICT policies. Our Security Specialists/ Network Administrators will:

- Install firewalls, anti malware software and access authentication systems. ● Arrange for security training for all staff.
- Inform staff regularly about new scam emails or viruses and ways to combat them. ● Investigate security breaches thoroughly.
- Follow this policy's provisions as other staff do.
- Our school will have all physical and digital shields to protect information.

When working remotely
Anyone working remotely for whatever reason, must follow this policy's instructions too. When staff are accessing our school's systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage staff to seek advice from our IT Administrators.

Reporting incidents, abuse and inappropriate materials
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other

policy non-compliance must be reported to the school's Data Protection Officer and Headteacher.

Disciplinary Action

We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal or written warning and train the staff on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, staff who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our staff and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.