Grace Academy Coventry

Critical Incident Policy and Procedure

Status	Operational
Authors	School Business Manager
Applicable to	All Staff, Trustees, Governors, Volunteers and Students
Checked by	Local Governing Body
Valid From	September 2025
Review Date	September 2027

Contents

Page

1 Introduction

1.1 Objective

The aim of this policy is to lessen the effect of a critical incident on the staff, students, other users, other premises and visitors and parents at Grace Academy. It is anticipated that by adopting the procedures outlined in this policy it will be possible to provide a more secure environment for everyone associated with the Academy.

1.2 What is a Critical Incident?

A critical incident is one which arises suddenly. Critical incidents may occur in or outside of the Academy, but in either circumstance have a major impact on staff and students. An incident might be designated as critical where the result is likely to be serious disruption to the running of the Academy, or where there is likely to be significant public and/or media attention on the Academy.

1.3 Examples of Critical Incidents

Inside the Academy:

- A serious accident to a child or adult
- The death of a student or member of staff through natural causes, such as an illness
- A traffic accident involving a student or staff member
- Violence or assault
- A fire or explosion
- Destruction of part of the building
- A major loss of critical services (e.g. power, IT) – see Appendix C
- Abduction of a student
- An illness such as meningitis within the Academy or the local community

Outside the Academy:

- An accident to a student, staff or volunteer whilst out of the Academy
- Death or injuries on an Academy journey
- Tragedies involving the local community
- Civil disturbances

1.4 Broadly speaking, incidents can be categorised as

- Incidents causing physical disruption to the premises

- Incidents that have a major impact on an individual or individuals and that have a consequent broader emotional impact.

2 When a Critical Incident arises

2.1 Procedures during an incident

- The Principal, or in their absence the Vice Principal, must be informed of any critical incident as soon as possible.
- If the emergency services have been called, their directions are to be followed at all times during the course of their involvement.
- As soon as an incident is confirmed, the Critical Incidents Team will meet to decide strategies.
- The Principal, or in their absence the Vice Principal, should inform the Trust and the CEO as soon as possible. The Chair of the Governors should be informed as soon as practically possible.
- The rest of the staff will be informed as soon as possible, preferably at a specially convened staff meeting. If information applies to volunteers the appropriate line manager should cascade this information as soon as possible.
- All staff should share the same information (subject to confidentiality requirements).
- Students will be told information simply and sensitively, without fabrication, preferably in smaller group situations.
- The Academy will try, as far as possible, to keep to the normal routine.

2.2 Critical Incidents Team (CIT)

The Academy has drafted a plan, taking advice from the police and other specialists to ensure that communication on site is effective should the need arise. The chair of the local governing body on behalf of the Trust should hold a copy of this plan. It is the responsibility of the Academy to forward a copy should the draft plan change at any point. A central component of this policy is the identification of the composition, roles and responsibilities of the Critical Incidents Team.

The role of the team is to review and direct the handling of the incident and the response and recovery process in order to:

- Ensure the safety and security of students, staff, other users of the premises and visitors.
- Minimise the loss to the academy in physical, human and financial terms.
- Manage an incident to minimise disruption to regular operations.
- Liaise with appropriate agencies, including the Media.

The Critical Incidents Team may comprise of the following personnel:

- Principal
- CEO
- Members of ALT
- Governors
- Other personnel may be co-opted on to the team as required

2.3 Action plan

Major incidents require the following procedures:

- Set up a communication network
- Convene the Critical Incidents Team
- Inform immediately the CEO, The Trust and the “Chair” of Governors and any other appropriate Officers.
- Collect, record and convey as much accurate information as possible
- Identify staff to receive incoming calls
- Office area to be used for enquiries
- Use the up to date list of students' next of kin (record files) and contact parents of affected children
- Record all actions
- In the first instance the Principal, alone is to act as 'press officer', with advice and instruction from the Trust
- Refusal of access to press/television on Academy premises

2.4 Obtaining information

It is essential to obtain and collate information about what has happened as soon as possible:

- What has happened?
- Where and when?
- Name and contact number of an adult at the incident site?
- Extent of injuries, numbers and names?
- Location of injured?
- Location of uninjured?
- What help is required?
- Who has been informed?
- What has been said?

3 Incidents Causing Disruption to Premises

3.1 What is the extent of the disruption?

The key factors to consider will be how much of the building, if any, continues to be operational, and how long the period of disruption is likely to last.

- In any significant disruption, e.g. fire or failure of critical services, health and safety of staff and students should be the key consideration.

- Contact should be made with key service providers and insurers as soon as possible.

- The CIT will need to consider whether to send staff and students home and for how long.

- Channels of communication with staff students and parents need to be maintained by use of telephone, web site and media, and where available and appropriate alternative forms of digital technology.

3.2 If total evacuation of premises is necessary

- Evacuate students to a safe area. This will probably be within the grounds of the Academy; however alternative locations are listed in Appendix B.

- Members of the ALT should be delegated to contact parents and ensure that students are safely handed over.

- If the premises are likely to be partially or totally out of use for a considerable time, the most likely course of action will be to establish temporary accommodation within the grounds of the Academy. Contact should be made with the RPA team who are likely to have a major incident team experienced in making such arrangements.

3.3 Major disruption to IT services

- The Academy manages its own IT services. Any disruption to service should be reported to the IT Support team in each Academy.

- We have a backup solution that is fit for purpose. All user/server data on all servers is backed up to a local backup NAS server and all virtual machine servers are backed up to the same backup NAS server via VEEAM. Staff are encouraged to save data directly to google and critical server data is automatically backed up to google on a daily basis, overnight.

- Full details are set out in Appendix C.

4 Dealing with a personal tragedy

4.1 First steps

- Contact families whose children are involved and families of any teacher involved. This responsibility might be best shared among members of the CIT or ALT once an agreed strategy has been taken. This must be done quickly and sensitively.

- Parents may want to come into the Academy. Appropriate support systems should be arranged (i.e. rooms and staff available).

- Make arrangements for informing other parents. Before doing this, careful thought should be given (and professional advice taken if necessary) about any legal liability, police action or health issue.

- Appropriate ways of informing parents might be a letter sent with students, a posted letter (if, for instance, an incident happens in the holidays) or a meeting at the academy. If the letter does not need to go at once, it may be better to wait until there is more information available.

- The Academy could be inundated with calls, e.g. anxious parents. There should be an agreed factual statement and reassurance of action being taken. Brief reception staff so that they are prepared to handle calls. Assign additional staff if necessary.

- Assume that news of the incident will reach the media. A statement should be prepared, and should then not be added to without the agreement of the CEO.

- Inform other staff and students. Careful consideration of the most appropriate way for this to be done is needed – this will depend on the circumstances. Students should receive a consistent account of the incident appropriate to their age and the degree to which the incident concerns people close to them.

- Inform the "Chair" of Governors, CEO and the Trust.

4.2 Next Actions:

- Develop a plan for handling the feelings and reactions of people. People's reactions will vary a great deal. Some will show feelings openly, others will not. Age will have some bearing on this. Denial, distress, guilt, anger or helplessness are all possible reactions.

- Be aware of the emotional state of students and staff. Encourage those involved to talk.

- Give guidance to the appropriate staff on how to talk to students. Be straightforward and take care with the form of words in announcements.

- Make clear the measures in place in the Academy to provide support for distressed children.

- Provide information to families on the kinds of help and support available to them and their children.

- Be aware that the incident may act as a trigger to students who are emotionally vulnerable for other reasons.

- Allow access to counselling. It may be necessary to call in external counsellors in certain circumstances. Parental permission should be sought in this instance.

- Staff closely involved with the students concerned should be offered opportunities for debrief and counselling.

- Anticipate further media interest.

- Inform the rest of the Governing Body (by an established cascade system).

- If the incident occurs in the school holidays and on an official Academy trip, all information submitted in advance by the trip organiser should be reviewed as soon as possible.
- Decide on formal and informal ways of recognising what has happened, such as:
    - Expressing sympathy to the families directly affected by the incident
    - Visiting anyone injured in hospital
    - Encouraging the sending of letters or cards
    - Attending a funeral
    - Holding a special assembly or memorial service
    - Being aware of anniversaries and handling them carefully.

- Continue or re-establish normal routines quickly and maintain the normal Academy day

- Be ready to assist and support students or staff who rejoin the Academy after an absence

5. Dealing with the Media

- The Principal will be the first point of contact for the media

- Be ready to deal with the media.

- The media may hear of an incident before the Academy and may have information that contradicts the Academy's.

- Police involvement may be needed to cope with excessive media attention.

- If the Trust is not available for signing off any statement, the Principal will be responsible for all communication with and response to the media. All other staff should avoid talking to the media unless specifically authorised by The Principal.

- An agreed text should be prepared for release to all staff (and students if appropriate) which anyone confronted by the media can speak from if it is unavoidable.

- Where possible, known contacts from the local media should be briefed.

5.1 Do's and Don'ts:

DO:

- Respond to "what" and "when" questions.

- Tell the story quickly and accurately and get the Academy's key message across.

- Consider, if possible, the needs of the audience.

- Choose your own time to report to the media.
- Make sure that everyone in the school has the same story.
- Prepare carefully.

DO NOT:

- Reply to “why” or “how” questions.
- Speculate.
- Bluff or lie.
- Make “off the record” comments.
- Make promises you cannot keep.
- Make excuses or blame others.
- Respond to blind quotes (“Another of your teachers has told me….”)
- Say “no comment”. Explain why you cannot comment.
- Allow words to be put in your mouth (“Would you agree …..?”)

All approaches from the media should be reported to The Principal and the member of staff or student should not respond to an enquiry but should redirect the enquiry to the Principal. Everyone needs to be alerted to the possibility that representatives of the media may use underhand tactics to get information or a response.

APPENDICES

6.1 APPENDIX A: Critical Incident Team – Contact Details

Grace Academy Coventry
Executive Principal: Mrs Natasha Whiles
Telephone: 02476 589 050

Associate Principal: Mrs Emily Wheller
Telephone: 02476 589 050

Tove Learning Trust
CFO: Mrs Sue Wagstaff
Telephone: 01327 320834

6.2 APPENDIX B: Alternative Locations

Alternative locations for evacuation of the academies in inclement weather or as circumstantially required:

Grace Academy Coventry
Wigston Road
Coventry
CV2 2RH

St Philips Church, Ringwood Highway, Coventry, West Midlands, CV2 2GF, contact tel. no. 02476 617 888.

6.3 APPENDIX C – ICT Specific

Critical Incident and Disaster Recovery (ICT Specific)

The following documentation addresses a variety of identified potential situations that may affect the functionality of the ICT systems across Grace Academy Trust.

Each Academy within the MAT have responsibility to ensure they have adequate policies and procedures in place, but may adapt the Trust model to maintain efficiency and protection.

System Backup

In the event of a critical event data must be in a format that it can be restored when required. Each Academy must maintain a regular backup of the system data. Two backups should be made, synchronised if possible. One should be onsite, away from the main servers, the other should be offsite. This can be Institution or Cloud based. It is recommended that a full backup is taken regularly. The minimum should be weekly with critical data backup daily. Where an academy uses services of a Cloud based service, the necessary information regarding to DR and DP should be passed to the Trust ICT Strategic Lead with details of DP to the DPO.

Backup facilities must be tested on a weekly basis and a report maintained. A DR is only as

reliable as the Data that can be restored. It the responsibility of the Senior Technician in each Academy to ensure that these backups are maintained.

Important

It should be noted that the following guide times and assessment are generic and should be considered for guidance only. It is the responsibility of the ICT Manager of Individual institutions to classify the following:

Chance of failure – risk assessment based on age and reliability of equipment. Risk will increase with age.

Downtime – risk assessment made against the support available within the ICT Team on site, ICT experience within the Trust and support available.

Whole School Power Failure

Chance of failure – Low Effect – Critical

Should the school suffer a complete power failure then power to all computers would fail. The servers have some protection through uninterruptible power supplies (UPS). This enables some time to down the services in an organised manner and would shut themselves down automatically after 30 minutes. The UPS's would safely shutdown the servers resulting in no loss of server data. All data from the desktops which has not already been saved to the servers would be lost.

A whole school power failure would result in the closure of the school until the situation was resolved. Once the power was restored then all the servers would need manually restarting. Full restoration with no data loss 15 mins.

Solution: There is no effective workaround to this problem. The CIT would need to liaise with the utilities power supplier to determine the seriousness of the problem and the downtime.

Downtime – Unknown

Partial power failures – Server Room

Chance of failure - Low Effect – Serious

Power failure in the server room would result in a loss of access to data systems hosted on the server and core switches.

Solution: The ICT is unable to resolve this without the third party intervention of utility supplier or electrician.

Downtime: - 2 hours

Failure of core Switches

Chance of failure - Low Effect – Varied

The core switches have redundancy features built-in, but it is still possible for them to fail totally.

Solution: Each of the core switches has redundancy built in to the switch plus there are two switches per function. Critical functionality could be re-patched into working parts of the network and bypassing any issues with failed switching equipment.

Downtime – 1 hour

Failure of Room Switches

Chance of failure - Medium Effect – Low

Failure of room based switches would cause limited data loss. This is isolated to the specified patching in place.

Solution: A room based switch is always held as a spare and used if required.

Downtime – 30 Minutes.

Failure of the Host(s)

Chance of failure - Low Effect – Critical

Failure of a virtual host would implement redundancy from the secondary host, since each academy should be running a n+1 configuration.

Solution: Guidance can be given within the ICT Trust Team

Downtime: 24 hours (with replacements required 48 hours to server uptime)

Failure of SAN

Chance of failure – Low/Medium Effect – Low

SAN1 is a storage area network device with multiple redundant parts including redundant hard disks, power supplies and network connections. A failure of the SAN completely would result in some servers being unavailable depending on which servers were hosted on that SAN.

Solution: Failure is unlikely and individual failure of redundant parts would have no effect. In the very unlikely failure of the SAN enclosure replacement would be implemented.

Downtime: 48 hours

Failure of Domain Controllers (names)

Chance of failure - Medium Effect – Low

The failure of a domain controller would have limited effect on functionality as the other DC's would take over its functions. We have enough domain controllers to continue working

Solution: Fix failed domain controller as soon as possible.

Downtime – None

Failure of Storage Staff or Student Server

Chance of failure - Low Effect – Medium

The failure of the Storage server would cause loss of access to student and curriculum based data that was not stored on the Google drive. All data is backed up daily, overnight, to Google without staff or student input.

Solution: Give temporary access to the backup server or host virtual server on different host until the Storage Server is fixed. Fix Storage server as soon as possible and restore data from backup server to Admin. Access to Google data could also be shared with staff/students as required.

Downtime – 2 to 3 hours

Failure of SQL

Chance of failure - Low Effect – High

Loss of SQL Database functionality including access to SIMS

Solution: Install SQL on another VM and restore the data for SIMS

Downtime – Within 24 hours

Failure of Phone System server

Chance of failure - Medium Effect – High

This would result in a loss of the internal phone system.

Solution: Whilst the server is recovered any calls to the school would be redirected to a mobile phone in reception or a personal mobile associated with a DDI.

Downtime – 15 mins

Failure through DOS or Malware

Chance of failure - Medium Effect – High

A denial of service (DOS) or a malware attack on a school is possible. A DOS would not significantly impact on the daily essential running of the Academy, however, a malware may. Each Academy should ensure that staff and students are adequately informed regarding potential threats and what to do. Sufficient AV software must be installed to protect against virus, but also malware.

Solution: The point of threat must be reduced as soon as possible. Where complete infection has occurred, the system must be considered inoperable and the CIT team consider the impact. The Senior ICT Technician should consult the ICT Strategic lead and the CIT about the programme for restoration. This will involve systematic rebooting and disinfecting where the point of entry is unknown.

Downtime: With support programme Essential systems 24-48 hours – Full system 3/4 days