Critical Incident Policy

Date Prepared	**February 2026**
Author	**Alison Moon**
Checked by (Trustee)	**Gavin Sibbick**
Date ratified	**31 March 2026**
Review date	**March 2028**

Contents

Aims

Veritas MAT recognizes the importance of a comprehensive Critical Incident policy to ensure the safety, security, and continuity of its data and operations. This policy outlines the procedures and responsibilities necessary to ensure safety for all and to recover and protect critical data in the event of a disaster, ensuring minimal disruption to our educational activities and administrative functions.

This policy has been formulated to ensure that any impact on business continuity, following any emergency situation such as flood, acts of vandalism or terrorism, pandemic, explosion, hardware/software failure, cyber-attack or any other disaster, is kept to a minimum.

This Policy will be supported by other plans and procedural documentation, dependent upon the type of incident, such as Cyber Security Policy and School specific Critical Incident Plans.

Definitions

Throughout this policy, the term incident will be used to reference any type of emergency/critical incident situation.

The Trust: Veritas Multi Academy Trust

The Registered office for Veritas Multi Academy Trust is:
c/o Warden House Primary School
Birdwood Avenue
Deal
Kent
CT14 9SF

The Trust Office is based at:
Mundella Primary School
Blackbull Road
Folkestone
Kent
CT19 5QX

The Trust has three schools:
Mundella Primary School, Folkestone
Pilgrims' Way Primary School, Canterbury
Warden House Primary School, Deal

This policy will apply to any schools joining Veritas Multi Academy Trust during the policy review cycle.

Trust Executive Leaders (CEO, Trust Business Manager and Governance Professional) and the Central Team (Executive Team Business Managers and Finance & HR Team) are equipped to work across sites and/or remotely enabling continuity in the event of a disaster at a school.

Scope

This policy applies to all data and information systems used by Veritas Multi Academy Trust, including but not limited to:

- Pupil records and academic data
- Financial and administrative data
- Employee records
- Learning management systems
- Communication systems

- IT infrastructure and hardware

It considers school practice in the event of critical incidents to ensure all schools have appropriate plans in place.

General Principles

(a) It will need to be identified whether an incident is Trust wide, such as a cyber-attack or a local event, as in the case of an intruder. Different types of incident will require different action. This Policy provides an overarching framework, supported by plans to support specific types of incident that account for local variance. Any incident must be alerted to the Trust Executive in order for assessment to be made as to whether it is a Trust wide or local event.

(b) In the event of a Trust Wide incident, such as cyber attack, the Central Team will co-ordinate and work collaboratively with school staff, carrying out liaison with external providers and media as required and supporting school staff with required communication tasks locally.

(c) Trust Leadership Team and the Central Team may support on site depending upon Critical Incident Categorisation & Levels, assessed need and safety.

(d) Trust and School Leaders will ensure that guidance referenced in the Academy Trust Handbook is considered and followed to maintain compliance. For example 'Meeting Digital and Technology Standards in Schools and Colleges.

(e) Schools are required to follow the Trust Technical Security Policy to mitigate the risk of malicious attack.

(f) Trust and School Leaders will engage with Internal and External Scrutiny processes as required.

Roles and Responsibilities

(a) In the event of a disaster, the Trust will convene a Critical Incident Response Team (CIRT). Key staff in the CIRT are:

- Chair of Trustees
- CEO (Chair and Critical Incident Controller)
- Trust Business Manager (Deputy Chair)
- Governance Professional, Company Secretary and Marketing Lead
- Exec Support Business Manager (Finance/Risk/Estates)
- Exec Support Business Manager (Office Team Lead and HR)
- Trust Site Lead/Local Site Manager
- Trust Network manager (This may be commissioned from IT contracted support)
- Headteacher & Safeguarding lead for school.

The CIRT will coordinate Critical Incident efforts across the Trust. In the event of a localised event, School Critical Incident Plans will be put in place. In this case, the Critical Incident Controller Chair and or Deputy **must** be contacted and further Central Support will be provided where appropriate.

The type of event may also lead to following specific plans as detailed below in section 6. It is required that all schools have the such plans in a format agreed by the Trust. These must be reviewed regularly as per review cycles.

(b) Administrative/Central Staff are responsible for

- Maintaining up to date records and documentation
- Assisting with communication and coordination during a disaster
- Supporting IT Support in data recovery efforts

(c) All employees of Veritas Multi Academy Trust are responsible for:
- Adhering to data security and back up protocols
- Reporting any issues or potential threats to IT support
- Cooperating with the CIRT and IT support during Critical Incident efforts

Critical Incident Mitigation and Procedures

(a) Critical Incident Risk Assessment - A Risk assessment will be conducted annually to identify potential threats to Veritas Multi Academy Trust and its schools, including an evaluation of natural disasters, cyber threats, hardware failures and other threats. The result of the risk assessment will inform the development and updating of the Critical Incident plan.
(b) Schools must adhere to all conditions stated in the DfE's Risk Protection Assurance Cyber Cover. This is detailed in the Technical Security Policy and Cyber Response Plan.
(c) All schools must engage in the development and implementation of the associated plans and documentation.
(d) All schools must engage in the development and management of Risk Management processes.

Incident Response

In the event of an incident, the following incident response procedures will be followed (see below for Incident Categorisation and Levels):

a. Detection & Initial Notification
- IT Support identifies a cyber incident, **or** another type of critical incident is reported.
- The discovering staff member notifies the Critical Incident Response Team (CIRT) immediately. The CIRT determines the incident level and contacts the Trust Leadership Team in the suggested time frame below when safe to do so.

b. Activate the Emergency Plan
- The CIRT leader activates the Emergency Plan.
- Roles and responsibilities are assigned (communications lead, IT lead, site lead, safeguarding lead, etc.).
- Immediate actions start to contain the incident, ensure safety, and maintain essential operations.

c. Communication with Stakeholders
- The CIRT issues updates to Staff, Students (where appropriate), Parents/carers, External agencies (police, IT security specialists, local authority, etc.)
- Messaging is kept consistent, factual, and appropriate for the incident type.

d. Assess Damage and Prioritise Recovery
- IT Support, Site Team, and/or the CIRT assess: Extent of damage, systems, data, or buildings affected and immediate risks
- The CIRT agrees on priority recovery tasks, such as: Restoring essential systems, securing compromised areas and ensuring safe continuation of school operations

Incident Categorisation & Levels

If you need assistance with any critical incident, contact the Trust Leadership Team as soon as it is safe to do so. If the situation is under control, refer to the table below for the required timeframe to notify the Trust Leadership Team.

Level	Description	Examples	Time to call Trust Exec Team
1	Minor	Power outage, minor injury	Within 24 hours
2	Moderate	Severe weather, building damage	Same day

3	Major	Fire, lockdown (non-threat to life), violent incident	Within 1-2 hours maximum
4	Critical	Cyber-attack, lockdown (threat to life) terrorism, death, mass casualty event	Immediately

Post-Recovery Review

Following an emergency incident, a post-recovery review will be conducted to evaluate the effectiveness of the Critical Incident efforts. The review will include:

(a) An analysis of the cause of the incident and its impact
(b) An assessment of the recovery process and timeline
(c) Identification of areas for improvement in the Critical Incident plan
(d) Recommendations for enhancing specific areas such as data protection and recovery procedures

Training and Awareness

To ensure preparedness, Veritas Multi Academy Trust will implement the following training and awareness initiatives:

(a) Critical Incident /Emergency Planning Training (CIRT and school staff)
(Including duty of care in the case of structural damage and environmental considerations and media/legal considerations)
(b) Awareness Campaigns: Regular Awareness Campaigns will be conducted to educate staff and pupils on various types of emergency preparedness such as cyber-attack, fire, bomb threat and intruder situations

Associated Plans and documentation

Completed Critical Incident documentation will be stored in SharePoint.

The following documentation is referenced in this policy and/or may be relevant in the event of a critical incident:

(a) Cyber Disaster & Response Plan (Trust)
(b) Technical Security Policy (Trust)
(c) Data Protection Policy (Trust)
(d) Schools Critical Incident Plan (Local) - *where relevant, the inclusion of partners on site, such as on-site nursery is required.*
(e) Critical Incident Risk Assessment
(f) Premises Management Policy