Business Continuity Policy

Item	Details
Policy Owner	Louise Morgan - CFOO
Review Level	Audit, Risk and Assurance Committee
Approval Level	Audit, Risk and Assurance Committee
Date Approved	October 2026
Effective Date	October 2027
Review Frequency	Annual
Next Review Date	October 2027
Version Number	2.0
Statutory / non-statutory	Statutory
Publication Location	Website / Governance Management / Internal

Checked By	Date
Executive Review	06/2026
Legal / HR Review (where applicable)	-
Governance Review	08/10/2026

Contents

1. Purpose and Scope 2
3. Governance and Responsibilities 4
4. Definitions 5
5. Critical Activities 5
6. Risk and Impact Assessment 5
7. Incident Types 5
8. Plan Activation 6
9. Incident Management Procedures 6
10. IT Disaster Recovery 6
11. Communication Strategy 6
12. Statutory Reporting 6
19. Related Policies and other documents 9

1. Purpose and Scope

The Balcarras Trust recognises the importance of effective business continuity planning in supporting the delivery of its strategic objectives and ensuring the continued provision of education and support services. Business continuity forms part of the Trust's wider risk management framework and helps ensure the Trust is able to respond effectively to, and recover from, incidents that may disrupt normal operations.

The Trust maintains appropriate business continuity arrangements to support the continuation of critical functions during periods of significant disruption. Where a Trust site becomes unavailable or unusable, essential operations will, wherever practicable, be relocated to suitable accommodation within another Trust school.

This policy sets out the Trust-wide arrangements for preparing for, responding to and recovering from incidents that may threaten the continuity of critical operations across the Trust.

This policy applies to all staff, all schools within the Trust, and all Trust-managed services.

The plan may need to be read in conjunction with the individual school's 'Emergency Response Procedure'. It is also worth noting that in addition to the Trust Risk register each school within the Trust will maintain a local risk register.

	Action	**Further Info/Details**	**Date Actioned**
1	Identify any other stakeholders required to be involved in the business continuity response	Depending on the incident, you may need additional/specific input in order to facilitate the recovery of critical activities. This may require the involvement of external partners	
2	Evaluate the impact of the incident	Take time to understand the impact of the incident on the normal operations of the Trust and its schools	
3	Log all decisions and actions, including what you decide not to do and include your decision making rationale	Activity log	
4	Log all financial expenditure incurred	Financial expenditure log	

5	Allocate specific roles as necessary	Roles allocated will depend on the nature of the incident and the availability of staff members	
6	Secure resources to enable critical activities to continue or be recovered	All IT systems to be backed up twice a day so that all records can be accessed even in the event of a Ransomware attack. The only risk to this would be a sustained regional powercut. Each school min the Trust should keep paper records of contact details	
7	Deliver appropriate communication actions as require	Ensure methods of communication and key messages are developed as appropriate to the needs of your key stakeholders	

Depending on the nature of the incident it might be that The Balcarras Trust would need to seek additional support, help or guidance. As a Multi Academy Trust our first resort would be to contact the Department for Education (DfE) Regional Director office for the South West. The RD has responsibility for all academy schools in the southwest. If we needed emergency support or help, for example, in securing temporary accommodation, then this would be the first avenue to explore. We might also need to contact the local authority depending on the nature of the incident. The Trust and each of its schools are members of the RPA Insurance Scheme for Academies.

3. Governance and Responsibilities

The Trust maintains a clear governance structure for business continuity, defining who activates the plan, who leads the incident response, and how escalation occurs to the Core Executive Team, Trustees, Regional Director, and external agencies.

Roles include:

Chief Executive Officer (CEO) – Strategic lead and final decision-maker

Chief Financial Operating Officer (CFOO) – Operational lead and policy owner

Headteachers – School-level incident leads

Governance Professional – Decision logging, compliance, and reporting

IT Lead – Cybersecurity and systems recovery

Site and Business Managers – Local operational support

Delegated authority levels and escalation thresholds will be maintained and reviewed annually.

4. Definitions

Incident – Any event that disrupts normal operations

Critical Activity – A function essential to safeguarding, statutory compliance, or Trust operations

MTPD – Maximum Tolerable Period of Disruption

RTO – Recovery Time Objective

These definitions ensure consistent understanding across all Trust schools.

5. Critical Activities

The Trust maintains a defined list of critical activities including safeguarding, communication systems, MIS access, payroll, Every, SEND provision, statutory reporting, and exam delivery.

Each critical activity has an assigned MTPD and RTO to guide prioritisation during an incident.

6. Risk and Impact Assessment

The Trust maintains a Trust Risk Register, and each school maintains a local risk register. Local Governing Bodies are responsible for reviewing local risks within their school and escalating any significant concerns to the Executive and, where appropriate, through the Audit, Risk and Assurance Committee (ARAC) to the Board of Trustees. The Trust Risk Register is prepared and maintained by the Executive and reviewed regularly by ARAC on behalf of the Board. The Board of Trustees retains overall responsibility for risk management and oversight of the Trust's risk profile.

Business continuity risks form part of the Trust's overall risk management framework and are considered alongside other strategic, operational, financial and compliance risks. This supports compliance with the Academy Trust Handbook and helps ensure that the Trust can continue to deliver its critical functions in the event of significant disruption

7. Incident Types

The following disruptions may significantly impact operations:

Loss of premises

IT failure, including ransomware

Loss of utilities

Loss of personnel

Loss of telecommunications

Loss of key suppliers

Additional risks may be identified through ongoing Trust-wide risk assessment.

8. Plan Activation

The CEO, CFOO, or Headteacher may activate the Business Continuity Plan when an incident threatens critical activities.

Staff must follow the relevant school's Emergency Response Procedure.

Activation triggers will be communicated clearly to all staff.

9. Incident Management Procedures

Identify stakeholders required Depending on the incident, additional internal or external partners may be required.

Evaluate the impact Assess the effect on normal operations across the Trust.

Log all decisions and actions Maintain a full activity log, including rationale for decisions taken or not taken.

Log all financial expenditure Maintain a financial log for audit and insurance purposes.

Allocate roles will depend on the nature of the incident and staff availability.

Secure resources All IT systems are backed up twice daily. The Trust also maintains offline and off-site backups to ensure resilience against cyber incidents.

Deliver communication actions Ensure key messages and communication channels are appropriate for stakeholders.

10. IT Disaster Recovery

The Trust maintains robust IT disaster-recovery arrangements, including offline backups, ransomware response procedures, and clear reporting routes for serious cyber incidents in line with DfE Cyber Security Standards.

Serious cyber incidents will be escalated to the ESFA and Regional Director where required.

11. Communication Strategy

A structured communication protocol sets out stakeholder groups, approved channels (email, SMS, website, social media), message sign-off procedures, and template messages.

Communication must be timely, accurate, and consistent across all Trust schools.

12. Statutory Reporting

Incidents meeting thresholds for serious incident reporting, safeguarding failures, cybercrime, or financial irregularities will be reported to the ESFA, Regional Director, or other relevant bodies.

The Governance Professional will ensure compliance with statutory reporting timelines.

13. Recovery and Resumption

The purpose of the recovery and resumption phase is to resume 'business as usual' working practises for the Trust and its schools as quickly as possible. Where the impact of the incident is prolonged, 'normal' operations may need to be delivered under new circumstances e.g. from a different location.

Agree recovery actions will be detailed in an action plan with timescales and responsibilities.

Respond to long-term support needs Counselling or wellbeing support may be required.

Communicate return to normal operations Staff will be briefed when the plan is no longer in effect.

Debrief staff and pupils Debriefing supports learning and wellbeing.

Complete an incident report Reviewed by the Core Executive Team and presented to Trustees.

Trustee review Trustees will review the plan in light of lessons learned.

Clear criteria will be used to determine when temporary arrangements end and how learning is embedded into risk management.

	Action	Further Info/Details	Date Actioned
1	Agree and plan the actions required to enable recovery of normal trust/school operations	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated	
2	Respond to any ongoing and long-term support needs of staff members and pupils	Depending on the nature of the incident, there may be a need to consider the use of counselling services	
3	Once recovery actions are complete, communicate the return to normal school operations	Ensure all staff members are aware that the business continuity plan is no longer in effect via briefing	
4	Debrief staff members (and possibly pupils) about the incident		
5	Complete a report to document opportunities for improvement and any lessons identified. This	The incident report should be reviewed by all members of the management team. Governors may also have a role in monitoring progress in completing	

	report should be read be overseen by the Core Executive team of the Trust (and the Senior Management Team of the individual School) and should be presented to the Trustees for approval	agreed actions to further develop the resilience of the school	
6	The Trustees should review this continuity plan in light of lessons learnt from the incident and the response to it	Implement recommendations for improvement and update this plan. Ensure any revised versions of the plan are read by all members of the management team	

13. External Support & Escalation

The Trust may seek support from:

Regional Director's Office

Local Authority

RPA Insurance Scheme

External support will be engaged where specialist expertise or emergency accommodation is required.

14. Important Contacts

Each School in the Trust is required to keep an Emergency Response Plan which is updated annually. This includes all of the relevant contact details in an emergency.
If any of our schools entered into a Business Continuity situation then the following information might be important.

The Trust's contact at the Department for Education (DfE) Regional Director office for the South West is:
Lucy Livings and Matt Stevens
Regional Department for Education (DfE) Directors
South West Regions Group
Second Floor
3 Glass Wharf
Avon Street
Bristol
BS2 0PS

rgsw.swindonwiltshireglouc@education.gov.uk

Gloucestershire Schools Critical Incident Support Team (Office hours):
01452 427547, 01452 328678, or 01452 328681

Senior Education Duty Officer (Out of hours monitoring):
07747 532852 (used if having difficulty reaching an officer during an out-of-hours school critical incident)

Risk Protection Arrangement

In the event of an incident the first thing to do is upload the potential claim to the DFE Risk Protection Arrangement Claims Portal

Portal and Contact Details

- **Online Portal:** rpaclaimforms.co.uk
- **Phone Number:** 0330 058 5566
- **Email Support:** rpa.cm@davies-group.com
- **Required Info to Submit:** Members Unique Reference Number (URN) or Membership Number

Tony Pickstock MCIPS
Risk Protection Arrangement Team| Commercial Lead
Operations Group | Commercial Directorate| Schools Commercial Team
Piccadilly Gate, Store Street
Manchester, M1 2WD
Mob: 07867469652
RPA.DFE@education.gov.uk

---

19. Related Policies and other documents

This policy should be read in conjunction with other Trust policies and procedures, including those listed below. The list is not exhaustive and should be considered alongside any relevant statutory guidance.

- Risk Management Policy
- Financial Procedures (including the Reserves Policy)
- GDPR Policy
- ICT Acceptable Use Policy
- Safeguarding and Safer Working Protocol and Procedures Policy
- Safeguarding Statement

- Emergency planning and response for education, childcare and children's social care settings - GOV.UK
- Keeping Children Safe in Education
- Working together to safeguard children
- promoting and supporting mental health and wellbeing in schools and colleges.