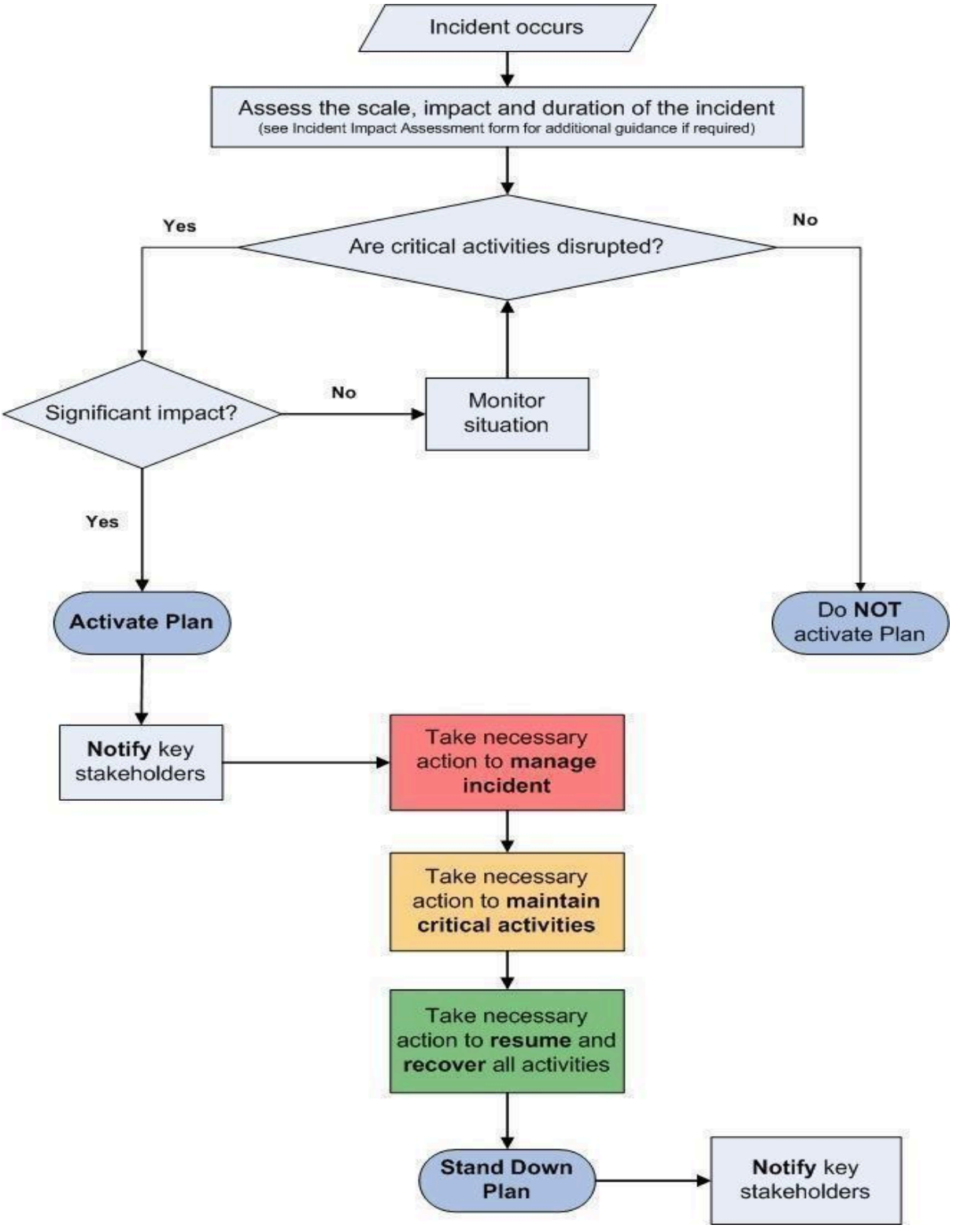
Name of Policy	**ICT Disaster Recovery Plan**
Responsible Body	**Trust**
Responsible Person	**COO**
Review Committee	**Finance and Resources Committee**
Last review date	Spring 2024
Next review date	Spring 2027
Revisions at last review	Updated to reflect Cheviot Learning Trust

CONTENTS	
A	PLAN ACTIVATION
B	INCIDENT MANAGEMENT
C	BUSINESS CONTINUITY
D	RECOVERY AND RESUMPTION

1.0 PLAN PURPOSE AND SCOPE	
Purpose	To provide a flexible framework to manage the response to any school disruption, maintain critical activities and recover from the incident quickly and efficiently.
Plan Scope	This is a whole Trust plan that supports all the Trust sites.
Links to other Plans and Procedures	This ICT Disaster Recovery Plan may be activated in the event of a highly significant disruption impacting on one/a number of schools.

2.0 PLAN ACTIVATION		
Circumstances	This plan is to be activated when a Trust site loses access to its ICT network. The aim is to recover operational capability as soon as possible and to prevent any loss or theft of data. There are many potential causes including equipment failure and cyber attack.	
Authority for Plan Activation	The most senior person on site would normally be responsible for activating the plan. Any activation of the plan must be advised to the Trust executive team via the COO.	
Notification Procedures	**Who?**	**Why?** (note this is NOT an exhaustive list)
	Headteacher	Take the decision on whether the Business Continuity Plan should be activated and direct resources. The Headteacher will normally be the 'Plan Owner'. See section 1.3 for more detail on plan activation.

2.1 PLAN ACTIVATION PROCESS



3.0 INCIDENT MANAGEMENT

3.1 INCIDENT MANAGEMENT PHASE

Purpose	Protect the safety and welfare of staff, visitors and the public Protect vital assets e.g. equipment, data, reputation Ensure urgent and necessary communication takes place Support the Business Continuity phase Support the Recovery and Resumption phase	If the disruption is not a 'no notice' emergency, section 4.0 will be of more relevance to you.

	REQUIREMENT	ACTION	ACTION DONE?	COMMENTS
1	Make a quick initial assessment: Survey the scene/situation Assess the impact on pupils and staff Assess (i.e. scale/severity, duration & impact)	Disseminate information (to others) Call the Emergency Services if needed Evacuate the school building if necessary	☐	
1a	Inform the Trust executive team and agree the resources required to manage the incident. Consider the requirement to inform insurers and obtain specialist support from the insurer. Consider what needs to be communicated to whom.	Create an incident response team and leader Allocate resources to the different aspects of the solution Create a communications plan		

2	TOTAL SERVER LOSS: In the event of total server loss due to fire or flood damage, new equipment will need to be sourced, quoted and ordered. (This will cause significant downtime as equipment needs to be built and delivered to site)	Source and obtain a quote for new equipment, send to school business managers for ordering.	▭	
3	SERVER BREAKDOWN (Hardware or HDD failure): In the event of a total hard disk failure, new drives must be ordered as soon as possible. In the event of total hardware failure, a new server will be required	Source and obtain a quote for new equipment, send to school business managers for ordering. Once new drives obtained, install and recover server from last backup state	▭	
4	Virtual Servers that can be hosted from temporary locations/hardware should be done as soon as possible to bring back core services to the network and allow end users to continue with work.	Identify an undamaged area of the school to set up and host virtual servers running core services, Active Directory, DNS, DHCP & Printing services.	▭	

5	Data will be saved to offline back up drives at each site and stored securely within a Fire proof storage facility within the grounds of the school.	Designated personnel must swap the offline backup devices weekly.	□	

4.0 BUSINESS CONTINUITY	
4.1 BUSINESS CONTINUITY PHASE	
Purpose	To ensure that 'critical activities' are resumed as quickly as possible and/or continue to be delivered during the disruption To activate one or more of your business continuity strategies to enable alternative ways of working To make best use of potentially limited resources by suspending 'non critical' activities
Time Critical Service Functions	The outcome of the Business Impact Analysis process has been to identify the following service activities as time critical/urgent: [Insert details]

	REQUIREMENT	ACTION	ACTION DONE?	BY WHO?
1	Take time to understand and evaluate the impact of the incident on 'business as usual' activities by communicating with key stakeholders to gather information. It may be useful to refer back to your Business Impact Analysis to review recovery time objectives and resource requirements for your most critical activities.	Depending on the incident, you may need additional/specific input in order to drive the recovery of critical activities. This may require the involvement of external partners.	☐	

2	Plan how critical activities will be maintained, utilising pre-identified or new business continuity strategies (see section 5.3 for your pre-identified strategies).	Consider: ● Immediate and ongoing priorities ● Communication strategies ● Resource availability ● Deployment of resources ● Roles and responsibilities ● Finance ● Monitoring the situation ● Reporting ● Stakeholder engagement ● Any welfare issues ● Planning the recovery of non critical activities	▫	
3	Identify any other stakeholders who may be required in the business continuity response	Depending on the incident, you may need additional/specific input in order to drive the recovery of critical activities; this may require the involvement of external partners.	▫	
4	Log all decisions and actions, including what you decide not to do and include your decision making rationale		▫	
5	Log all financial expenditure incurred as a result of the incident		▫	

6	Deliver appropriate communication actions as required	Ensure methods of communication and messages are developed as appropriate to the needs of your key stakeholders e.g. Pupils, Staff, Partners/Carers, Governors, Suppliers, Local Authority, Central Government Agencies etc.	▫	

4.2 BUSINESS CONTINUITY STRATEGIES	
Purpose	To document alternative ways of working designed to maintain your critical activities in the event of a disruption To ensure alternative ways of working have been agreed, tested and are fit for purpose
Circumstances when business continuity strategies may be activated	Whatever the cause of disruption, the impacts will generally be one or more of the below categories: Loss of critical systems e.g. ICT network disruption, telephony outage, power outage, utilities disruption, third party supplier disruption etc Denial of access, or damage to, facilities e.g. loss of a building through fire or flood, an external emergency where emergency service cordon would prevent access for a period of time, utilities failure etc. You may also require the activation of continuity arrangements in the event of an office move Loss of a key resource such as an external supplier or partner vital to the delivery of a key activity

TACTICAL OPTIONS TO MITIGATE AGAINST A LOSS OF PREMISES		ADDITIONAL INFORMATION
1	Identification of alternative locations designated as the agreed 'work area recovery site'. You will need to consider transport requirements and accessibility for these identified premises. You may need to have multiple places agreed for your work area recovery if you have large premises and these different options will need to be documented. You may find it helpful to categorise available sites according to the following: • 'cold' sites - has no equipment/furniture/computer systems set up but can be re-fitted in the event it is needed. This obviously means it takes longer to make 'fit for purpose' following an incident. • 'warm' sites - usually these sites will have hardware and connectivity already established though may take some time to be fit for purpose. • 'hot' sites - is essentially a duplicate of the original site, with full computer systems as well as near complete back-up of user data, but may not match the capacity of the original site.	
2	Mutual support agreements with schools where there is capacity for schools to accommodate each other in the event of an incident.	
3	Virtual learning environment opportunities	
4	Localising the incident, e.g. isolating the problem and utilising different sites or areas within the school premises portfolio	

TACTICAL OPTIONS TO MITIGATE AGAINST A LOSS OF CRITICAL ICT SYSTEMS (INCLUDING TELEPHONY)		ADDITIONAL INFORMATION
1	Flexible lesson plans	
2	Use of a secure external network, virtualised network or secure cloud that can be accessed via the internet to allow extra backup and protection for your files.	G SUITE (GOOGLE DRIVE)
3	Manual workarounds: ensure there is a record of where pre-printed forms etc are stored and that there are procedure guides to inform their use where necessary.	
4	Access systems via the internet outside of your network for secure, cloud based applications.	GOOGLE G SUITE (DATA)
5	Ensure that anyone who requires ICT to undertake critical activities has the ability to work at home where possible and appropriate. Ensure that critical equipment is taken home where practical and possible and consider procuring mobile equipment for these users.	
6	Using different ways of working. This could include: changing work patterns, suspending 'non critical' activities to focus on your priorities and assist the recovery of critical systems in the first instance with a phased approach for all other ICT 'non critical' activities.	

5.0 RECOVERY AND RESUMPTION PHASE	
Purpose	To return to 'business as usual' as quickly as possible To ensure any non critical activities suspended as part of your business continuity response are recovered within appropriate timescales Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building on a longer term basis.

	REQUIREMENT	ACTION	ACTION DONE?	COMMENT
1	Agree and plan the actions required to enable recovery and resumption of normal working practices.	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated.	▫	
2	Continue to record all expenditure incurred as a result of the incident.	Use the Financial Expenditure Log to record any expenditure	▫	
3	Respond to any ongoing and long term support needs of Staff and Pupils.	Depending on the nature of the incident, the schools Incident Management Team may need to consider the use of health services, for example counselling.	▫	
4	Once recovery and resumption actions are complete, communicate the return to 'business as usual'.	Ensure all staff are aware that the Plan is no longer in effect.	▫	

5	Carry out a 'debrief' of the incident with Staff and Suppliers/Partners if appropriate. Complete a post incident report to document opportunities for improvement and any lessons identified.	The incident debrief report should be reviewed by all members of the Schools Incident Management Team to ensure that key actions resulting from the incident are implemented within designated timescales.	▫	
6	Review this Business Continuity Plan in light of lessons learned from the incident and the consequent response to it.	Implement recommendations for improvement and update this Plan.	▫	
7	Veaam backup software is deployed to servers at the KEVI Site, Chantry & Newminster Site backing up to Network Attached Storage Synology devices. Data will (also) be saved to offline back up drives at each site and stored securely within a Fire proof storage facility within the grounds of the school.	First point of call for these sites is to refer to the Veaam backups for recovery options. Where necessary, recover from the previous backup drive?...	▫	