MANCHESTER CITY COUNCIL

NEWALL GREEN PRIMARY SCHOOL BUSINESS CONTINUITY PLAN

PLAN DETAILS	
Date Written	17 November 2025
Plan Owner	Headteacher (Sarah Rudd)
Plan Writer	SLT (Alec Killingbeck)
Review Schedule	6 monthly ☐ Annually ☒
Date of Plan Review	Annual review, with contact lists updated every six months
Date of Plan Exercise	
Plan Storage Details	

VERSION CONTROL		
Date	**Change Details**	**Approver**

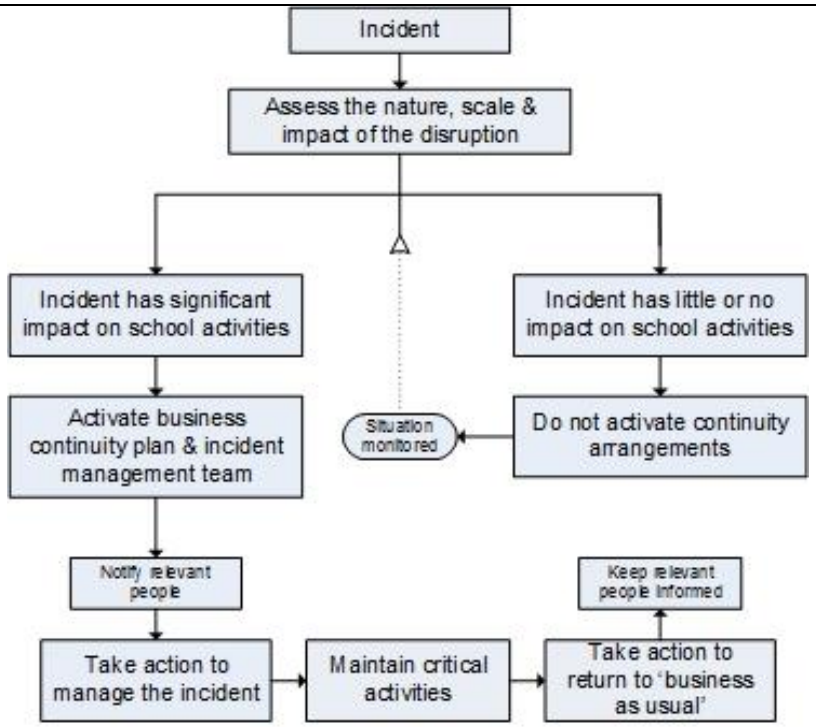
1.0 PLAN PURPOSE AND SCOPE	
Purpose	To provide a flexible framework to manage the response to any school disruption or major incident, maintain essential school activities and recover from the incident quickly and efficiently.
Plan Scope	Applies to all staff, pupils and visitors across EYFS, KS1 and KS2 mainstream provision, the 12-place resource provision, 30-place SEN unit and 12-place alternative provision.
Links to other Plans and Procedures	Links to Critical Incident Policy Hard-copy grab bags should be stored on site near an evacuation point and off site to ensure access if the premises or ICT systems are unavailable. All members of the incident management team should hold a secure copy of this plan.
2.0 PLAN ACTIVATION	
Circumstances & triggers	This plan will be activated in response to any incident that causes significant disruption to the delivery of normal school activity, particularly teaching and safeguarding. Typical triggers include: • **Loss of staff or skills** – above-normal absenteeism due to illness, injury or severe weather preventing travel. • **Loss of critical systems** – ICT network disruption, telephony outage or power failure. • **Denial of access or damage to facilities** – fire, flood, structural failure or external emergency cordons. • **Loss of key resources or suppliers** – failure of meal provision, transport, specialist therapists or other essential partners. • **Widespread disease outbreak** – significant illness requiring school closure or remote learning; contact Public Health England for advice.

	• **Information security breach / cyber attack** – suspected data loss or malicious activity affecting systems or confidentiality.
Authority for plan activation	The Headteacher is responsible for deciding whether to activate the plan. In their absence a Deputy or nominated senior leader will do so. The first member of the incident management team on site will coordinate the response until the Headteacher or deputy arrives
Plan Activation Process	At the onset of an incident, take the following steps to facilitate timely decision-making and protect life: 1. **Survey the scene** – assess the nature, scale and severity of the incident; ensure the safety of pupils, staff and visitors; evacuate if necessary. 2. **Assess impact** – consider which departments or classes are affected, including specialist provisions; account for all persons and identify casualties or injuries. 3. **Call emergency services** if required. 4. **Disseminate information** – brief the incident management team and staff; determine whether to close all or part of the school; initiate communications to parents and the Local Authority. 5. **Start an incident log** – record decisions, actions and the rationale behind them; note any staff or pupils injured and any property losses. 6. **Nominate roles** – assign individuals to carry out incident management roles (see Section 6).

3.0 INCIDENT REPORTING

Who?	**Why?** *(note this is **not** an exhaustive list, communication will vary on the circumstances of the event)*	
Emergency Services	Call 999 if the incident needs an urgent emergency response If your incident relates to an imminent terrorist threat to life or property, please contact the Police on 999 or the Anti-Terrorist Hotline on 0800 789 321.	
Headteacher or Deputy	The Head is responsible for taking decisions on appropriate incident response e.g. whether business continuity arrangements should be activated and direct resources to respond. The Headteacher will normally be the 'Plan Owner' and will lead the incident management team.	
Board of Governors	The Board is responsible for overseeing strategic decisions in response to significant incidents in coordination with school senior management. If the incident involves suspected malpractice or fraudulent activity, staff should follow the reporting routes set out in the Whistleblowing Policy and Anti-Fraud Policy.	
Key stakeholders such as staff, parents/carers and partners	If the incident is causing significant disruption, an appropriate message should be released to relevant stakeholders/partners detailing: ▪ Event details and the impacts ▪ Action being taken to respond to the incident ▪ Estimated length of the disruption and return to business as usual. ▪ When and how further information will be provided Consider the timeliness of any messages as well as the most appropriate channels and the sign-off process.	
Manchester City Council (most up to date contacts available on the Schoolshub Wesbite)	'Civil Emergency' Number	[redacted]- available 24/7 365 days per year Can be used to report an emergency incident that puts people in immediate danger, such as a collapsing building or bridge, an explosion or severe flood. This should only be used in an extreme emergency situation; the Council's emergency control centre may be activated in response. Emergency services will also activate the emergency arrangements if they determine this is necessary.

	Media Response	[redacted]
	Significant Building Incident	
	Serious accident or injury	
	Extreme Weather (e.g. snow) and School Closures	
	Information Security Breach	
	Any other type of major incident and in the event that the above contacts are unavailable (e.g. terrorist attack, serious criminal activity, death of a pupil or staff member)	
Public Health	In the event of a significant outbreak in a school, Public Health England (PHE), who lead the investigation and management of outbreaks and incidents, should be contacted. The Public Health England GM Health Protection Team can be contacted in/out of office hours: [redacted].	
ESFA	In the event of suspected financial loss, fraud or irregularity over £5000 or unusual/systematic patterns regardless of value the ESFA should be notified on	
4.0 INCIDENT RESPONSE FRAMEWORK		



5.0 INCIDENT MANAGEMENT

Initial response	▪ Quickly assess, review and verify key facts ▪ Survey the scene, ensure health and safety of pupils, staff and visitors ▪ Risk assess situation - scale, severity impact and duration of the event ▪ Notify emergency services as appropriate ▪ Evacuate the building if necessary, or is it safer to stay? Consider assembly points/evacuation arrangements. Ensure recording processes are in place for staff/pupils leaving the site ▪ Communicate according to criticality – notify and escalate as needed ▪ Consider roles & responsibilities needed to respond to the incident ▪ Refer to experience from similar previous incidents where possible ▪ Discuss, prioritise and disseminate actions ▪ Ensure a log of key decisions and actions is started and maintained throughout the incident ▪ Where appropriate, record names and details of any staff or pupils that may have been injured or affected by the incident as part of your incident record keeping, including material losses ▪ Assess the key priorities for the remainder of working day/next day and take relevant action
Ongoing considerations for incident response, continuity and recovery	▪ Welfare issues for those affected by the incident ▪ How will we maintain our critical school activities? What are our key priorities? Will we need to close school? How quickly can it be re-opened? ▪ Activate our contingency plans for a loss of staff, building, ICT, supply chain… ▪ Incident monitoring and reporting ▪ How will we return to 'business as usual'? Consider recovery and salvage if appropriate ▪ Communications – staff, management, parents/carers, partners, public and the media, including social media. Engage Council Media Team as needed. ▪ Reporting to Governors, Manchester City Council and other school stakeholders ▪ Consider resourcing any out of hours response ▪ Keep a log of key decisions and actions ▪ Resources - short, medium and long term arrangements, availability and

	deployment. Depending on the incident, you may need additional/specific input from your external partners and suppliers. ▪ Finance / insurance issues – protect vital assets and log all expenditure ▪ Respond to any ongoing or long term support needs of staff and pupils ▪ Ensure incident records are collated and stored securely ▪ Carry out a post-incident debrief with staff and suppliers, partners as appropriate – document any learning from the incident and any actions to help prevent re-occurrence or mitigate risks and vulnerabilities ▪ Review business continuity plan in light of incident learning
6.0 INCIDENT MANAGEMENT ROLES AND RESPONSBILITIES	
Role	**Responsibilities**
Incident Manager/ Incident Management Team	▪ Determining overall response and recovery strategy ▪ Activating and standing down incident response arrangements ▪ Safeguarding the welfare of all pupils, staff, contractors and visitors ▪ Ensuring key stakeholders are kept informed during an incident and in the recovery phase – pupils, parents/carers, staff, Local Authority etc ▪ Prioritising the recovery of key activities disrupted by the event
Incident loggist	▪ Ensuring that all key decisions, supporting rationale and all actions taken in relation to the incident are recorded clearly, accurately and stored confidentially ▪ Ensuring all incident records are collated and are able to withstand scrutiny e.g. Public Enquiry
Caretaker/Facilities Management	▪ Undertaking duties to ensure site security and safety in an incident ▪ Advise on any issues relating to physical infrastructure of the building ▪ Lead point of contact for any Contractors who may be involved in incident response ▪ Support the incident management team in creating an inventory of any damaged assets/equipment when/if safe to do so
First Aider	▪ To ensure that the Emergency Services are immediately called when they are required to treat any casualties ▪ To provide immediate first aid to casualties in line with training received to preserve life, prevent the condition getting worse and to promote recovery ▪ To keep individuals as comfortable as possible until professional help arrives
Fire Safety Responsible Person	▪ Emergency evacuation and coordination ▪ Point of contact, ability to provide floor plans to Fire Service ▪ Invoking Personal Emergency Evacuation Plans (PEEPs) ▪ Dynamic risk assessment
7.0 BUSINESS CONTINUITY STRATEGIES	
Purpose	▪ To ensure that time critical school activities are resumed as quickly as possible and/or continue to be delivered during the incident with pre-prepared or dynamic workarounds ▪ To document alternative ways of working designed to maintain your critical school activities in the event of a disruption ▪ To ensure alternative ways of working have been agreed, tested and are fit for purpose
Incident Type	**Response options**
Loss of premises or partial loss	▪ As we have a large site – initially the first decision would be to see if we can use alternative areas within school and move children to an existing area in school. ▪ Alternative building(s) – Potential to use St Paul's High School and Newall Green Dixons Academy should we need to, with a priority being for Year 6. – Due to the number of children for the whole school, this would not be a feasible long-term option. For this, portacabins would be the last option.

	▪ Contact to be made with Aspens to arrange how meals can be made elsewhere and brought to where the children are ▪ Emergency 'grab bag' that contains essential information and equipment needed for both incident management and business continuity. Essential resources should be should be stored in a secure place on and off site. ▪ Virtual learning environment opportunities – Use of Teams if appropriate ▪ Ensure that anyone who requires ICT to undertake essential activities has the ability to work at home where possible. ▪ Consider site security and safety at all times.
Loss of staff or skills	▪ Use of temporary staff (teaching/non-teaching) ▪ Multi-skilling/cross training/to ensure staff can undertake different roles and responsibilities where appropriate. ▪ Use of pre-prepared educational materials that allow for independent learning where appropriate ▪ Team activities and sports to accommodate larger numbers of pupils at once ▪ Larger class sizes (subject to relevant ratios) ▪ Ensuring that the business continuity aspects of staff management are considered in management arrangements e.g. flexibility in job descriptions ▪ Engage resources to support students/pupils and staff dealing with emotional impacts in the case of injury, accident or death where appropriate
Loss of ICT or telephony	▪ Teaching using manual methods ▪ Use of a secure external network, or secure cloud that can be accessed via the internet separate to the school to allow extra back up and protection for our files ▪ Records are stored on Arbor, so where needed can be accessed via the internet (e.g. on mobile phones) ▪ Redirection of the reception phone line to an alternative number or SLT mobiles though the 3CX Admin Account ▪ Ensure that One Education have given assurance regarding back up processes for our data and have a Disaster Recovery Plan that sets out the service they will provide to us in the event of a failure of their system
Loss of utilities (including water/gas/electricity)	▪ Document utility provider information – including emergency numbers ▪ In a power cut, call freephone number 105 that will put you through to our local electricity network operator. Switch off all electrical appliances that shouldn't be left unattended, ready for when the power comes back on. ▪ To report a gas or carbon monoxide emergency or if a pipeline is struck (even if no gas leak has occurred) call [redacted] 24 hours a day ▪ If our water supply is interrupted by an emergency, such as a burst main water pipe, our water company must restore the supply within 12 hours of becoming aware of the problem. However, if it's in a strategic main pipe, they must restore the supply within 48 hours. Our water company must take reasonable steps as soon as possible to let us know where we can get an alternative water supply, when it plans to restore the supply, a telephone number where we can get more information. ▪ Specific advice will be available from your our providers – contacts are: **Water:** **Electricity:** **Gas:**
Severe weather event such as snow, heat, high winds or flooding incidents	▪ Ensure monitoring arrangements in place for severe weather events, Met Office and Environment Agency provide trusted forecast information and flood alerts so that additional contingencies can be put into place where necessary. ▪ These types of incident will usually impact premises, staffing, ICT or all of the above, so re-consider whether the above options would be fit for purpose if we are developing specific plans and arrangements for severe weather events. ▪ We will use the school website and School Spider, to inform parents in

	advance of any severe weather incidents, and if they occur while in school, we will also use contact details to call where necessary.
Terrorist response and other major emergencies	Please refer to the Critical Incident & Emergency Response Policy ▪ Report all suspicious activity to the Police ▪ https://www.protectuk.police.uk/ produce a range of advice on the steps to keep safe in the rare event of a terrorist attack, including a short 'stay safe' video with 'Run, Hide, Tell' principles ▪ ProtectUK is a new counter terrorism awareness product from NaCTSO designed to provide specific advice and guidance on identifying security vulnerabilities, responding to suspicious behaviour, dealing with a suspicious item, bomb threats and firearms and weapon attacks. ▪ Save the Children Take Care Toolkit is a great resource to involve pupils in emergency planning to help build resilience ▪ www.manchester.gov.uk/mbcf - for ongoing business continuity support

Cyber attack	**The following advice should be read in conjunction with the schools Online Safety Policy** **1. Preparation (Before an attack)** **Objective:** Reduce the risk and ensure you're ready to respond. • Make sure you have an up-to-date inventory of systems, data, users and access rights. This aligns with the NCSC "10 Steps to Cyber Security" advice on asset inventory and secure configuration. NCSC+2NCSC+2 • Ensure security controls are in place: strong passwords, multi-factor authentication, up-to-date patches, filtering of malicious content (phishing emails) — for example via Get Safe Online and Cyber Aware guidance. Met Police+1 • Define clear roles and responsibilities: who is the SLT digital-lead, the IT support lead, the data protection officer (DPO), who reports to governors/trustees, etc. • Develop and document an incident response plan (for cyber attacks) as part of your business continuity / disaster recovery planning. According to schools-specific guidance you should have one. SWGfL+1 • Ensure you have reliable, tested backups (and preferably offline/air-gapped copies) of critical systems/data and test the restores. SWGfL • Train staff and students to recognise cyber risks (e.g., phishing emails, suspicious links) and to report issues promptly. The "meet digital and tech standards for schools" guidance emphasises awareness. GOV.UK+1 • Ensure you know how to report incidents externally: e.g., via Action Fraud (for UK) and NCSC schools guidance. NCSC+2UK Parliament+2 **2. Detection & Initial Response (When you suspect an attack)** **Objective:** Act quickly to contain damage and gather information. • **Identify**: As soon as staff or students spot something unusual (e.g., locked systems, ransom note, unusual account activity, large data transfer, weird network behaviour) the incident must be flagged to IT support and SLT digital lead. • **Contain**: Decide immediate actions — e.g., disconnect affected systems from network, isolate compromised accounts, change access credentials. • **Preserve evidence**: Don't immediately wipe logs or shut down everything unless absolutely necessary; record what you see (timestamps, symptoms, who noticed it). This is important for follow-up and possibly legal/police actions. • **Activate incident response plan**: Follow the pre-documented steps, engage IT support (internal and external), notify appropriate roles (SLT digital lead, DPO, business manager). • **Communicate internally**: Inform staff that an incident is being managed, advise them what (if anything) to avoid doing (e.g., using certain systems, opening suspicious emails) until further notice. **3. Recovery & External Reporting** **Objective:** Restore operations safely, mitigate harm, comply with obligations. • **Recover systems**: From backups if needed, ensure systems are clean before reuse, apply patches, change passwords, ensure no persistence of attacker. • **Notify external bodies**: ○ If data breach of personal data: consider reporting to the Information Commissioner's Office (ICO) within 72 hours (UK) if required.

	○ Report the incident to Action Fraud (for live attack / cybercrime) if your school is the victim. Action Fraud ○ Report via the NCSC schools incidents page if applicable. NCSC+1 ○ Where a cyber incident results in actual or suspected financial loss, fraud, or irregularity, the Trust must follow ESFA reporting requirements as outlined in the Anti-Fraud, Corruption & Cybercrime Policy, including notifying ESFA of losses over £5,000 or unusual/systematic patterns regardless of value. • **Communicate externally**: If appropriate (parents, students, staff, regulators) — but ensure communications are clear, factual, avoid panic, and approved by senior leadership. • **Review & learn**: After the incident, hold a debrief: what happened, how it was handled, what went well, what needs improvement. Update your incident response plan accordingly. • Cyber incidents with suspected fraud, data loss, ransom, or financial risk must also be escalated to the Executive Headteacher and Trust Business Manager as per the Anti-Fraud Policy. • Where a cyber incident suggests misconduct, fraud, or policy breach, evidence must be preserved and handed over to the Executive Headteacher and Trust Business Manager for investigation under the Fraud and Corruption Policy and the Trust's Disciplinary Procedures. **4. Longer-Term Actions & Prevention** **Objective:** Strengthen your school's cyber security posture to reduce future risk. • Use the NCSC's "10 Steps to Cyber Security" framework as a roadmap to embed good practice across the organisation. NCSC+2NCSC+2 • Carry out periodic risk assessments: what assets you have, what threats, what controls. • Ensure software/devices remain patched, software configurations are secure, user privileges are limited (i.e., don't give all users admin rights) — key points in the NCSC guidance. NCSC+1 • Ensure strong network defences: firewalls, intrusion detection/monitoring, filtering of malicious content. • Regularly test your backups and your incident response plan (e.g., table-top exercises). • Educate students and staff constantly: embed 'cyber awareness' as part of school culture (acceptable use policies, training, reminders). The schools' standards emphasise that. GOV.UK • Consider certification or adherence to minimum standards such as Cyber Essentials (government-backed scheme) to demonstrate you are doing the basic controls. GOV.UK+1 **5. Quick-Reference Checklist for an Incident** • Immediately alert: IT support + SLT digital lead. • Disconnect/Isolate affected systems if needed. • Record all relevant details (time, what, by whom). • Do *not* delete logs or evidence unless authorised. • Restore from clean backup if required. • Change compromised credentials. • Report externally (Action Fraud, ICO if data breach, internal governing body/trustees). • Communicate internally to staff. • After recovery, review what happened and update our plan.

8.0 INCIDENT COMMUNICATIONS PLAN	
Initial response and ongoing considerations	▪ Incident reporting arrangements – who, how, when? ▪ How will you establish key facts and agree messages? ▪ Do you have any pre-agreed messages, holding statements available? ▪ Who needs to sign-off incident communications? ▪ Which communication channels are available and how will you use them? E.g. school website, answer phone. Don't forget that communication channels can be compromised - include contingency measures ▪ Consider media response early on, including social media and how this will be managed and coordinated with other key stakeholders. Consider school spokesperson and ensure training in place. ▪ Which stakeholders do you need to provide updates to? ▪ Do you have relevant contact information available? ▪ Remember to monitor social media/listen to feedback

APPENDIX A: KEY CONTACTS - NOT TO BE PUBLISHED ONLINE

STAKEHOLDER KEY CONTACT LIST	
Contact	**Telephone number**
School Contacts	
Headteacher	[redacted]
Deputy Head	[redacted]
Premises Manager	[redacted]
Chair of Trustees	[redacted]
Chair of Governors	[redacted]
Deputy Chair of Governors	[redacted]
Other Local Contacts	
Police	[redacted]
Police – your local station/community officer	
Greater Manchester Fire & Rescue Services	[redacted]
Hospital – your nearest A&E	[redacted]
Your Local Church or Religious Centre	
BBC Manchester	[redacted]
NHS – your local clinic	
Other Useful Contacts	
Department for Education	[redacted]
Foreign Office	[redacted]
Public Health England	[redacted]
Information Commissioner's Office	[redacted]
Health and Safety Executive	[redacted]
United Utilities	[redacted]
Electricity North West	[redacted]
British Gas	[redacted]

APPENDIX B: GRAB BAG

The purpose of the 'grab bag' is to provide you with easily accessible critical information or equipment that you would need in a major incident all in one place. Grab bags are particularly useful in the case of loss of premises or loss of ICT. The below list are suggestions of what you can include in this - however each school will have different needs and this is not a prescriptive. Some of the key forms referenced here are available on the extranet if you find them useful, others can be developed by you to suit your own purposes.

Essential Items	
Details	**Why?**
Pupil registers/absence sheet/pupil numbers sheet	Accurate pupil records are vital to ensure that in the event of evacuation or relocation pupil safety can be ensured
Medical Notes (records of medication requirements) for pupils	To ensure that pupils health and wellbeing is maintained wherever education provision is taking place
Business Continuity Plan	To ensure good practice is followed when responding to an incident and to ensure the plan is accessible in the event of an incident.
Incident Impact Assessment Form	To assess the impact of the incident in order that the appropriate action can be taken in managing the response.
Lost Property Form	To record the details of any possessions staff, visitors or pupils have lost or have left behind as a result of the incident. This can assist with insurance claims.
Financial Expenditure Log	To record any expenditure made in connection with the incident e.g. costs of emergency supplies purchased etc. This form only records the additional expense generated by the incident which may need to be referred back to e.g. if an insurance claim is made.
Injuries And Fatalities Log	This information may be required for use by the emergency services, as well as by management. This information will also be required for insurance purposes to ensure policy conditions are met.
Post Incident Report	Following an incident it is essential that a 'debrief' takes place with staff, pupils and Suppliers/Partners, if appropriate. The incident debrief should capture what went well, plus opportunities for improvement and any lessons identified. The debrief is also a way of assessing any staff or pupil welfare requirements following an incident that need to be addressed.
Evacuation Procedure	In the event of an incident requiring evacuation, the safety of all those within the building is paramount and it is therefore vital that your agreed evacuation procedure is followed.
Assets Register (including ICT assets)	In the event of a loss of building incident e.g. due to fire or flood it is useful to have a record of assets to assist in the insurance claim.
Insurance Risk SLA	Includes general conditions summary
First Aid Kit	To assist in providing immediate first aid in line with training received in order to preserve life, prevent the condition getting worse and to promote recovery.
Stationery – e.g. pens, paper	Particularly important to allow recording a record of events in the incident particularly in the event of a loss of ICT
Additional Items	
Details	**Why?**
Utility supply location information/isolation tap	This can be useful information when there has been an incident impacting your school premises, such as a fire or

	flood and you need to switch the supply off urgently.
Floor plan showing evacuation routes	In the event of a fire or violent attack/terrorist attack this can be useful information
ICT equipment, for example laptop	This may be useful in the event of an ICT network outage. You may also wish to keep copies of software licence agreements and key codes, if appropriate.
Office telephone list	In the event of an incident requiring relocation, this information may be required for phone diverts.
Mobile phone, mobile phone charger and battery powered charger/power pack.	To mitigate against a loss of telephony, a mobile phone is a useful contingency. In the event of a loss of power, a battery powered charger will help to ensure communication with key stakeholders can still take place. It is helpful if the phone has a camera, as an emergency incident may become part of a crime scene and photographs may be useful evidence. Ability to listen to the radio and internet access may also be valuable to keep you up to date with the news - especially if the school's incident is part of a wider geographical incident. A battery powered charger can be difficult to source so a useful alternative can be a powerpack/bar. Although this needs to be charged initially they can then hold the charge for a longer period so can be used to charge a phone in a power cut situation.
Greater Manchester A – Z map	To assist in any logistical aspects required as part of the incident response especially in the event of a loss of internet access.
LED torch (preferable wind up)	In the event of a loss of power, particularly in the winter months you may find a torch useful. If possible to source a wind up torch this helps in the event that the batteries have run down.
High visibility vest	This is a form of personal protective equipment and it may be an easy way to ensure those directly managing the incident are clearly visible.
Hazard barrier tape	This may be useful if only part of a building is affected by an incident and you need to cordon-off part of the site for safety reasons – on the advice of the relevant professionals.
Whistle/megaphones	In the event of an incident requiring emergency evacuation or invacuation, this may be useful in managing a large crowd.

APPENDIX C: INCIDENT LOG

LOG OF EVENTS, DECISIONS AND ACTIONS			
Completed by		Sheet Number	
Incident Overview		Date	
Time	Log Details		

Appendix D (Staff contact list) and E (parent and carer contact list) – Up to date versions can be obtained through Arbor