Business Continuity Plan

GASCOIGNE PRIMARY SCHOOL

Gascoigne Road
Barking
London
IG11 7DR

Approved by:	Full Governing Body	**Date:**	29/09/2025
Signature (Chair of Committee):	Abidah Kamali	**Signatures (Co-Headteachers):**	James Fox & Anre Buchner
Last review date:		**Next review date:**	September 2026

A copy of the policy will also be available in:

- The Staffroom
- The Head's office
- School's web site

This will ensure that the policy is readily available to visiting teachers, support staff and parents.

REVIEW PROCEDURES

This policy will be reviewed regularly and revised as necessary.

Any amendments required to be made to the policy as a result of a review will be presented to the Governing Body for acceptance.

Related policies:

The following should be read in conjunction with this policy:

- Health & Safety Policy
- Critical Incidents Policy
- Disaster Network Management Policy

Objectives

This Business Continuity Plan details procedures to ensure the continued operation of the School in the event of an interruption to normal ICT department services, including providing the ability to successfully recover Information, Business Systems and ICT Equipment in the event of a disaster.

Objectives of the plan are

I. to ensure preventive measures are in place which reduce the risk of loss of Management Information Systems and ICT Equipment.

II. to ensure that action is taken to mitigate the consequences of any incident affecting Management Information and ICT Equipment

III. to give detail of any temporary arrangements to be made in the event of a Major Incident/disaster affecting the ICT Management information Systems and ICT Equipment.

Using this Business Continuity Plan will minimise confusion, errors, and expense to the School and will help effect a quick and complete recovery of services. In addition, it will provide on-going protection for school assets (equipment and information).

Risk management and School policy

The school has a Critical Incidents Policy which gives details of the procedures which would be undertaken in relation to potential disasters.

The Critical incidents management team (CIMT) is comprised of the following –

- **Directors of Operations** – James Fox and Anre Buchner (Co-Headteachers)
- **Communications Directors**
  Paul Vickery (Deputy Head) Media liaison;
  Richard Puttnam (Strategic Business Lead) Emergency services liaison
- **Director of Site Operations** – Mikey Morrissey (Premises Manager)
- **Governor Liaison** – Eugenie Augustin (Office manager)
- **Minute Taker** – Eugenie Augustin (Office manager)

ICT Response Team

The purpose of the ICT Response Team is to establish and direct-action plans to be followed in the event of a Major/Minor Incident. The ICT response team will involve the CIMT along with Danny Fitch (IT Co-ordinator - Curriculum) and Jack Taylor (IT Technician)

Organisation and planning

The ICT Response Team will be formed accordingly to respond to the Incident. It will be dependent on the severity as to which members of the team would be needed. The Incident Co-ordinator will usually be the Director (ICT).

The position of Director can be delegated appropriately according to the nature of the incident but it must be clearly established exactly which member of staff is the Director of Operations at the start of the process of dealing with any incident. This must also be detailed as part of the record of the incident.

This policy will be enhanced with clear procedures which cover a number of critical incidents e.g. off-site evacuation, lockdown, snow day and fire etc.

ICT Alternate Site

In the event of a major disaster, an Alternate Site will be used from which all communications, recovery operations and activities will be directed. The alternate site is either:

Gascoigne Primary School	Gascoigne Primary School

Gascoigne Road Barking Essex IG11 7DR	The Shaftesburys Barking Essex IG11 7JA

Business Continuity Plan.

The full list of School systems will be held by the school's ICT Support Service (Elementary ICT).

Elementary ICT constantly monitor their Helpdesk so that any reported incident or issue is addressed promptly. Elementary ICT will either resolve issue themselves or will collaborate with third party providers where appropriate and necessary.

If the problem is with an administration system then the School Business Manager should be notified.

A. Replacement equipment

If ICT systems are damaged or destroyed or the Server Room is unavailable, necessary hardware and software will need to be procured quickly and delivered to the Server Room or the Alternate Site. The school will purchase replacement equipment through existing arrangements with vendors and funds will be made available.

B. Back ups

The pupil MIS system (Arbor) is cloud hosted, administered and backed up off site by Arbor Education. It is web-based so service can be restored quickly. The finance system (e5) is administered by the Local Authority, it is monitored, supported and backed up by their team.

The school network is backed up via Veeam to a Network Attached Storage (NAS) unit on the Gascoigne Road site, SharePoint is backed up via Barracuda to an off-site cloud location which is separate from Microsoft's Azure infrastructure. In the event of a fire that destroys the server and backup equipment, the backup copies in the cloud can be used to quickly restore to a new system.

C. Copies of Key Documents

To ensure that key documents are available in the event of an incident the School retains a copy of this Plan along with any key documentation (such as pupil, staff and LA emergency contacts) including up to date administration paperwork in 'grab bags' in the main school office.

D. Theft

All school ICT equipment is security marked in line with the borough systems. In the event of a theft the police should be notified immediately and the appropriate steps taken to resume daily running of the school with the minimum of disruption to all stakeholders.

E. Power Outages

If the school suffers from a power outage paper documentation is held in the main school office. Hard copies of emergency contact numbers and pupil parent details are also kept in the grab bags. The school also holds a hard copy of all Critical Incident Emergency policies and procedures. The server room and school's admin systems are protected by an Uninterrupted Power Supply (UPS) which will support operations during briefest routine power outages (30 minutes at most and allow the servers to gracefully shut down if UPS battery runs out charge).

F. Major Incident

To be read in conjunction with the school's Critical Incidents Plan.

To ensure that essential **paper records** can be recovered in the event of a Major Incident (excluding fire) the members of staff responsible for each area would collect the documentation before leaving the site.

If the major incident is a fire and the school needs immediate evacuation all administration systems are web based and can be accessed from any computer or smart phone outside of the school premises. All members of the Senior Leadership team along with Elementary ICT are contactable on mobile phones and have access to devices.

All virtual servers are backed up to a Network attached storage (NAS) device using Veeam Backup and Replication software to the alternative site. Offsite cloud backups for all shared data are stored on a Barracuda data centre. Backup details are in the Network Disaster Recovery document.

The school would be evacuated to the alternative site where there would be access to a hot desk with a computer.

All administration documentation (MIS and Finance) is web based and services could be accessed by us from the evacuation site to enable the school a minimum level of functionality.

G. Procedure for Network Failures

Elementary ICT will determine the scope and severity of the failure or outage. Where possible, temporary replacement parts or re-routing of data services will be provided until the appropriate replacement parts become available. In the event that the cable plant has been compromised every effort will be made to restore service as quickly as possible.

H. Procedure for Hardware Failures

In the event of a system failure, Elementary ICT will determine whether the failure is hardware or software related. Hardware failures generally require either repair or replacement if equipment is still under warranty. Hardware should be able to be repaired sufficiently quickly to restore operation within

several hours. If replacement is required, the relevant procedures would be undertaken to ensure hardware is restored swiftly.

The Deputy Headteacher is responsible for all curriculum hardware replacements and the School Business Manager is responsible for all administration hardware replacements.

I. Procedure for Software Failures

Operating System software is typically under maintenance from the vendor. If a failure is software related, the ICT contact will work with the vendor's technical support staff to correct the problem in a timely manner for any curriculum software and the School Business Manager will deal with administration software. Vendor Contact details are held by the ICT Team.

J. Procedure for System Failures

Most of our systems are purchased from third-party vendors and these companies are often responsible for the maintenance of the systems. Some have been developed or highly customised and are now maintained by the ICT department. In-house change control procedures provide for adequate testing before making changes and for backing out the changes if problems are detected. However, a more serious type of application failure is one where, through error of a program, a user, or other means, data is compromised to the degree that business consequences are serious.

In this case, the ICT contact must determine how the erroneous data will be corrected, with possible assistance from the application software vendor.

Allowable outage times for each system or ICT resource will be necessary.

Testing and Maintenance of this Plan

Testing

The following areas should be addressed in a test:

. System recovery on an alternate platform from backup media
. Coordination among recovery teams
. Internal and external connectivity
. System performance using alternate equipment
. Restoration of normal operations
. Notification procedures

. Classroom exercises: Participants in classroom exercises walk through the procedures without any actual recovery operations occurring.
. Functional exercises: Functional exercises require the event to be simulated, there may be actual interagency and vendor participation. A functional exercise might include actual relocation to the Alternate Site and/or system cutover.

Test results and lessons learned should be documented and reviewed by the Critical Incidents Management Team along with the designated IT managers. Information collected during the test and post-test reviews that improve plan effectiveness will be incorporated into this Plan.

Training for personnel with Business Continuity Plan responsibilities should be provided and updated whenever there is a change to the Plan. New members of staff who will have plan responsibilities should receive training shortly after they are hired. Responsible staff should be trained to the extent that that they are able to execute the appropriate procedures without aid of the actual document. Recovery personnel should be trained on the following plan elements:

. Purpose of the Plan.
. Cross-team coordination and communication.
. Reporting procedures.
. Security requirements.
. Team specific processes.
. Individual responsibilities.

The Critical Incidents Management team will ensure that the ICT Response Team and other employees receive appropriate training and will ensure that new employees are properly trained.

Maintenance

The Critical Incidents Management team is responsible for evaluation and updates of this ICT Business Continuity Plan to assure that appropriate contingency plans have been prepared for relevant emergency situations. This will be part of the annual review.

Changes to information about ICT systems will be documented and disaster recovery measures revised if required.

Contact lists will be revised when required. Plan reviews will focus on the following elements:

. Operational requirements
. Security requirements
. Technical procedures
. Hardware, software and other equipment
. Names and contact information of team members or vendors
. Alternate site facility requirements

This Plan contains potentially sensitive operational and personal information and its distribution is restricted to relevant members of the ICT Department and other Key Staff.