Batchwood School

make every day count

BUSINESS CONTINUITY PLAN

Kerry Pollard

Kerry Pollard

……

Signed – Governor

……

Print Name

Date: November 2017 **Review:** November 2018

To provide guidance to school staff, governors and external parties on how to react to disruption – major or minor.

1. Rationale

1.1 To ensure the core purpose of the school, teaching and learning, is continued with as little disruption as possible.

1.2 To ensure the continuance of network operation or the swift return of ICT network capability in the event of a disruption –major or minor- to the running of the system.

2. Aims

2.1 To ensure all key personnel are contacted and know what to do in the event of an incident likely to lead to minor or major disruption to service.

2.2 To assist in the planning of future developments to improve business continuity.

2.3 To provide an aid to risk assessments that might need to be made.

2.3 To ensure that a plan exists to put the school back into service in the event of an incident.

3. Procedures & Details

3.1 A copy of this document is to be stored off-site by the following people who will form the emergency response team. Provisional responsibilities are suggested below:-

Role	Name	Position	Home Tel	Mobile
Overall responsibility	Jonathan Kemp	Headteacher		
Responsible for communications and students	Jonathan Kemp Lisa Harvey Catherine Russell	Headteacher Finance Manager Heads PA		
Responsible for curriculum and teaching staff	Laura Graham Kelly Vincent	SLT SLT		
Responsible for premises and support staff	Ross Whitaker Debbie Hawkes	Deputy Headteacher Lead TA		
Responsible for network	SITSS Lisa Harvey	 Finance Manager		
Responsible for managing premises/health and safety	Amanda Clewlow Tom Tansey	Health & Safety Manager SLT		

3.2 The emergency response team will base itself in the main reception offices and the Headteacher's office unless this area is out of action. An alternative location would be the School Hall.

3.3 Chain of command will be:

- Headteacher Jonathan Kemp
- Deputy Headteacher Ross Whitaker

3.4 Key services that must be maintained:

Essential function	Duties	Staff required first week
Finance	Accurate record keeping, salaries, financial commitments	2
HR	Support for staff	1
Premises	Site open and safe to function	5
Administration	Attendance Examinations	1 3 1
Toilets	Safe and working toilet facilities for male and female	1
Water	Running – hot and cold	1
Canteen	Drinks, refreshments	1
Database	County/DfE returns	2

3.5 Key holders

Name	Position	When to contact	Address	Contact Numbers
Jonathan Kemp	Headteacher			
Ross Whitaker	Deputy Headteacher			
Tom Tansey	Site Manager			

3.6 ICT and Finance – see annexes on detailed ICT and Finance guidance.

3.7 Temporary accommodation will be provided as follows in order to provide essential services if an incident prevents access to the normal place of work.

Department		Temporary Location
English		Heathlands School, St Albans
Maths		Heathlands School, St Albans
Science		Heathlands School, St Albans
Art/music		Heathlands School, St Albans
Technology		Heathlands School, St Albans
Examinations	Heathlands School, St Albans	

4. Communications

4.1 In the event of a serious incident care must be taken when liaising with the public and press. All communication will be directed through the Headteacher, or, in their absence, the next in line of command and shown in 3.3. HCC press office (01992 588535) should be contacted to ensure messages are reasonable and robust to protect individuals and the school.

4.2 Every attempt will be made to ensure accurate and timely information is provided to families and staff. This will be coordinated by the emergency response team and use the usual system for school communication as shown below:

4.3 In the event of a serious incident, all staff and students affected by the same will have the opportunity to access counselling services organized by the school, should they so wish.

Type of Communication	Responsible	Contact
Website	Katie Harris	info@katewatkiss.co.uk
Parent mail	Catherine Russell	07788 416844
Telephone tree	Jonathan Kemp	07896 311974
Herts. School Closure List	Catherine Russell Lisa Harvey Amanda Clewlow	07788 416844 0798 123 450 07425606626

5. Other Information

5.1 Paper based records are available which duplicate IT based documents and some hard copy only documents.

Document	Location	Duplicated	Responsible
Finance	Current and previous year (s) in School office cupboard	On Server Remote backup	Lisa Harvey
Student details	In student files – School offices Old files in archive room	On Server Remote backup	Catherine Russell
Staff details	In locked filing cabinet in school office	On Server Remote backup	Lisa Harvey Amanda Clewlow
Governor minutes	In locked cupboard in school office	On Server	
Health and Safety Records	School Office	On server Remote Backup Files in office	Amanda Clewlow
Audit Reports	School office	Finance Office On Server Remote Backup	Amanda Clewlow
County/DfE statistical returns	School office	Finance Office On Server Remote Backup	Lisa Harvey
Student results and performance	Headteacher's office	On Server Remote Backup	Jonathan Kemp Katie Harris
Staff Performance Management	In locked file in Headteacher's Office		Jonathan Kemp

5.2 External Contacts are listed below. This list is not exhaustive but highlights key and regular contacts with the school.

Organisation	Purpose	Name of Key Contact	Tel No.	Out of Hours	Other Info
Emergency Services	Major emergency – large scale		999		
Gas Emergency	Loss of gas or leak				www.systems-link.com/webreports
Electricity Emergency	Loss of electricity or major failure				www.systems-link.com/webreports

5.3 Office inventory

Item	Head's Office	School Office	Head of Wellbeing office		Deputy Head office	
Computers	1	4	1		1	
Desks	1	4	1		1	
Chairs	1	4	1		1	
Scanner		1				
Printer		2			1	
Photocopier		1				
Telephone	1	4	1		1	
Security Camera system			1			

ICT & Payroll Disaster Recovery Plan Appendix to BCP		
Last Reviewed: January 2017	**Next Review: January 2018**	

Purpose and Scope

- Introduction
- Objectives/Constraints
- Assumptions
- Incidents Requiring Action
- Contingencies
- Physical Safeguards
- Types of Computer Service Disruptions
- Insurance Considerations

Recovery Team

- Disaster/Recovery Team Headquarters
- Disaster Recovery Co-coordinator

Preparing for a Disaster

- General Procedures
- Software Safeguards

Recovery Procedures

- Degraded Operations at Central Site
- Network Communications

Telephony - Disaster Recovery (Appendix A)

- Background
- Backup and Restore Procedures
- Disclaimer

Purpose and Scope

Introduction

Batchwood School Trust has a paper and computerised operational environment. This includes the use of servers, PCs and peripherals across the whole site. A school-wide network ties these various systems together and provides communications to other computer networks. In addition, the operation of the School network provides a vital support component of the School system.

The reliability of computers and computer-based systems has increased dramatically in the past few years. Computer failures that do occur can normally be diagnosed and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continual operation when some failures occur.

The infrastructure design has resilience, with built-in network redundancy, enhancing our ability to cope with a major disaster. Failure of part of the network would not necessarily disable the remainder of the site.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to the computing systems. The various situations or incidents that can disable, partially or completely, or impair support of Batchwood School's computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the School in order to allow the affected systems to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery.

Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting different departments in Batchwood School's technology areas. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the School, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to Batchwood School and the administrative systems within the remit of the IT and the ICT Coordinator. Batchwood School uses SITSS external support for IT issues and we are supported weekly. Our manager is James Toll. Offices at Batchwood School should develop their own internal plans to deal with manual operations should computer and/or network services be disrupted.

Assumptions
This section contains some general assumptions, but does not include all special situations that can occur. Any special decisions for situations not covered in this plan needed at the time of an incident will be made by appropriate staff members on site.

This plan will be invoked upon the occurrence of an incident.

The senior staff member on site at the time of the incident or the first one on site following an incident will contact the Finance Manager for a determination of the need to declare an incident. The Headteacher will also be notified.

The senior staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. Batchwood School's Admin Office will be notified. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., **but** evacuation is the highest priority.

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and the relevant authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable computer and/or telephone support to the School has been re-established.

Incidents Requiring Action

The ICT disaster recovery plan for Batchwood School can be invoked under one of the following circumstances:

1. An incident which has disabled or will disable, partially or completely, the School Network facilities for a period of 24 hours.
2. An incident which has impaired the use of computers and networks managed by SITSS due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems.
3. An incident which was caused by problems with computers and/or networks managed by ICT and has resulted in the injury of one or more persons at Batchwood School.

General situations that can destroy or interrupt the computer network usually occur under the following major categories:

- Power/ Interruption
- Fire
- Water
- Weather and Natural Phenomenon
- Sabotage and war
- Theft

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - operating at an alternate site and/or other client areas within the School.
- Full recovery - operating at the current site and client areas, possibly with a degraded level of service for a period of time.

Physical Safeguards

The serve at Batchwood School is protected by lockable doors in the Gold Room. The Site have access to the keys. The room is protected by fire alarms.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve Batchwood School's Networking facilities. Some minor hardware problems do not disrupt service; maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

Major telephone problems

Problems regarding outside telephone lines are the responsibility of BT. Batchwood School is responsible for the upkeep and maintenance of the internal telephone system, which has been installed by Avaya.

Environmental problems (electrical, fire)

Electrical

In the event of an electrical outage, all servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPSs). Once electrical power is restored the servers will remain "powered down" until the UPSs are recharged a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure.

Fire

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware. Our critical data is backed up daily.

Insurance Considerations

All major hardware is covered under Batchwood School's standard insurance for the School.

Recovery Team

1. If the Main Site is usable, the recovery team will meet in the Headteacher's Office.
2. If the Main Site is not usable, the team will meet at School House.
3. If the alternative site is not usable, the team will liaise by mobile phone.
   If none of the School facilities are usable, it is presumed that the disaster is of such proportions that recovery of computer support will take a lesser priority.

ICT Disaster Recovery Coordinator

The IT manager/Finance Manager will serve as ICT Disaster Recovery Coordinator. The major responsibilities include:

- Determining the extent and seriousness of the disaster, notifying the Headteacher and immediately and keeping them informed of the activities and recovery progress.
- Invoking the ICT Disaster Recovery Plan after approval.
- Supervising the recovery activities.

- Coordinating with the Headteacher on priorities for staff and students while going from partial to full recovery.
- The Headteacher will keep staff and students informed of the recovery activities.

The Finance Manager in conjunction with SITSS and SLT will be responsible for:

- Coordinating hardware and software replacement with the academic hardware and software vendors.
- Coordinating the activities of moving backup media and materials from the off-site security files and using these for recovery when needed.
- Keeping the Headteacher informed of the extent of damage and recovery procedures being implemented.
- Coordinating recovery with individual faculties, contractors and hirers.
- Coordinating appropriate computer and communications recovery regarding Offsite Backup

Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

Maintaining and updating the ICT disaster recovery plan.

- Ensuring that the SLT team are aware of their responsibilities in case of a disaster.
- Ensuring that periodic scheduled rotation of backup media is being followed.
- Maintaining and periodically updating ICT disaster recovery materials, specifically documentation and systems information, stored in the off-site areas.
- Maintaining a current status of equipment.
- Ensuring that UPS systems are functioning properly and that they are being checked periodically.
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that proper temperatures are maintained in server areas.

Recovery Procedures

This portion of the disaster/recovery plan will be set into motion when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time.

It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. This decision will be made by the Headteacher/ upon advice from SITSS and the Finance manager.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify SITSS that a priority should be placed on assistance to add and/or replace any additional components.
- Order any additional electrical cables needed from suppliers.

- Rush order any supplies, forms, or media that may be needed.
- In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:
- Notify the Site Manager that an alternate site will be needed for an alternate facility.
- Coordinate moving of equipment and ICT support personnel into the alternate site.
- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine the priorities of the client software that need to be available and load these packages in order. These priorities often are a factor of the time of the month and academic year when the disaster occurs.
- Prepare backup materials and return these to the off-site storage area.
- Set up operations in the alternate site.
- Coordinate school activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage periodically.
- Work out plans to ensure all critical support will be phased in.
- Keep administration and staff and students informed of the status, progress, and problems.
  Coordinate the longer range plans with the administration, the site officials, and staff for time of continuing support and ultimately restoring the overall system.

Network Communications

Since most of the telephone and computer communications lines are buried and in conduits across School, connecting lines to alternate sites and to critical areas cannot be done rapidly.

Payroll Disaster Recovery

Payroll is processed off site by the outsourced provider, SERCO. Payroll preparation is completed by the Finance Manager and this is then sent to SERCO Payroll for processing. The process can be completed manually if necessary.

Telephone - Disaster Recovery

In the event of a serious incident resulting in the loss of telephone communication the alternate means of direct communication for key personnel will be via personal mobile phones as listed:

1. Headteacher: Jonathan Kemp
2. Deputy Headteacher Ross Whitaker

Emergency Response Plan last updated: January 2018. Plan last tested December 2017 with snow closure.

Appendix A

Background

The IT computer network consists of 1 Server. The whole site has both wired and wireless connectivity.

Backup and Restore Procedures

The following documentation gives details of procedures for the recovery of data in circumstances where a catastrophic loss of data has occurred due to file server failure. There are a variety of reasons for file server failure including hardware/software conflicts and failure, accidental or deliberate damage, hacking and inexplicable failures normally called ‘Act of God failures'. The latter probably can be tracked to a specific cause but it is rarely worth the time and effort required.

Backups are carried out by SITSS automatically every evening.

Disclaimer

While every effort is made to ensure the integrity and security of data held on the network, the Network Team cannot accept responsibility for permanent loss of data arising from any cause. Users should, at all times, follow standard network usage procedures: particularly maintaining regular local copies of important files.