



***Information Systems (IS)
Continuity Plan***

For

Charlton County Schools

Version: Phase I (Central Office)

Date Created: 6 February 2006

Updated: 7-17-2018

The information contained herein is copyright protected under the title

Business Continuity Plan Generator™ (U.S. Version)

IS Continuity Plan	2
IS 010102 Benefits of Developing an ISCP	3
IS 010103 ISCP Policy Statement	4
IS 020101 Environmental Disasters	4
IS 020102 Organized and/or Deliberate Disruption	5
IS 020103 Loss of Utilities and Services	6
IS 020105 Serious Information Security Incidents	7
IS 020106 Other Emergency Situations	9
IS 020304 Key IT and Communications Suppliers and Maintenance Engineers	12
IS 020303 Key IT Personnel and Emergency Contact Information	13
IS 020302 Key IT, Communications and Information Processing Systems	14
IS 020305 Existing IT Recovery Procedures	15
IS 020403 External Emergency Services and Contact Numbers	16
IS 020502 Back-up Power Arrangements	17
IS 030201 Functional Organization Chart	18

IS Continuity Plan

Charlton County Schools recognizes that threats could exist that may damage or destroy the ability to continue normal business operations following a serious unexpected disruptive incident. The organization has a high level of dependency upon its automated systems and processes and this creates risks that need to be mitigated.

We also recognize that we need to recover from disruptive incidents in the minimum possible time consistent with safety, good order, and discipline. The necessity to ensure speedy restoration of services requires a significant level of advance planning and preparation.

The best defense against catastrophe is in following good day to day work practices and being aware of both internal and external environments. If done well, many 'disruptive events' will never occur.

This IS Continuity Plan has been prepared to assist the organization to manage a problem that affects our information systems in a controlled and structured manner. It contains information on emergency contact details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to an emergency.

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 010102 Benefits of Developing an ISCP

Charlton County Schools understands the reasons why an ISCP is necessary. These are listed below.

- Increased recognition of the impact that a serious incident could have on our day to day operations
- Increased dependency by Charlton County Schools on computerized information systems
- Need to establish a formal process to be followed when a disaster occurs
- Need to develop effective backup and recovery strategies to mitigate the impact of disruptive events
- An intention to minimize costs and losses arising from serious incidents

ADDITIONAL COMMENTS:

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 010103 ISCP Policy Statement

A successful ISCP project depends on receiving a high level of support from Senior Management.

The following ISCP Policy Statement reviewed and approved by the Superintendent of Schools.

<ul style="list-style-type: none">➤ The organization should develop a comprehensive IS Continuity Plan.➤ The Director of Information Systems will take the lead in developing the ISCP and will have the responsibility for keeping the plan up to date.➤ A risk assessment should be undertaken in order to determine the requirements for the IS Continuity Plan.➤ The IS Continuity Plan should cover all essential and critical business activities.➤ The IS Continuity Plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergencies and that the management and staff understand how it is to be executed.➤ All staff must be made aware of the IS Continuity Plan and their own roles in developing and implementing the plan.➤ The IS Continuity Plan is to be kept up to date to take into account changing circumstances.
ADDITIONAL COMMENTS:

THIS POLICY STATEMENT WAS COMMUNICATED TO ALL MANAGEMENT AND STAFF ON 2-14-2006 and annually reviewed

IS 020101 Environmental Disasters

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

The ISCP Project Team has examined each potential environmental disaster or emergency. The focus here is on the level of business disruption, which could arise from each type of disaster.

Potential environmental disasters assessed as follows.

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	IMPACT RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Fire (catastrophic)	4	3	Interruption of business processes for >72 hours
Hurricane	2	3	Interruption of business processes for >72 hours
Tornado	3	2	Interruption of business processes for >48 hours
Lightning	2	3	Interruption of business processes for >8-12 hours
Damaging wind	3	3	Interruption of business processes for >8-12 hours
Tropical Storm	2	3	Interruption of business processes for >48 hours

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY HIGH	1	TERMINAL
2	HIGH	2	DEVASTATING
3	MEDIUM	3	CRITICAL
4	LOW	4	CONTROLLABLE
5	VERY LOW	5	IRRITATING

IS 020102 Organized and/or Deliberate Disruption

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

Each potential disaster or emergency posing significant risk resulting from 'organized disruption' considered. The focus in this table is on the level of business disruption that could arise from each type of disaster.

Potential disasters resulting from 'organized disruption' assessed as follows.

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	IMPACT RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Theft	5	4	Interruption of business process for >48 hours, until replacement equipment is on site.
Internal 'attack'	5	3	Interruption of business process for >72 hours, until replacement equipment is on site, investigations begun, legal actions are clear, etc.
Civil unrest	4	3	Interruption of business process for >48 hours, until situation has stabilized and personnel and equipment are deemed safe.
Terrorism	4	2	Interruption of business process for undetermined time, until situation has stabilized, personnel, and equipment deemed safe.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY HIGH	1	TERMINAL
2	HIGH	2	DEVASTATING
3	MEDIUM	3	CRITICAL
4	LOW	4	CONTROLLABLE
5	VERY LOW	5	IRRITATING

IS 020103 Loss of Utilities and Services

COMPLETED BY	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
REVIEWED BY	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

Each potential disaster or emergency situation resulting from loss of utilities and services was also considered. The focus is on the level of business disruption that could arise from each type of disaster.

Potential disasters result of loss of utilities and services assessed as follows.

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	IMPACT RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Electrical power failure	3	3	Without power, computers, lights, air conditioning, telephones, and other communication medium will not be operational.
Loss of water supply	5	4	Likely to close premises until the supply is restored. Possible health and safety issue as minimum sanitary needs cannot be met. Often caused through a fault in a water supply route.
Air Conditioning	4	4	Environment affects both human and machine resources. Heat beyond machine specification will result in shutting down equipment.
Telecommunications loss	4	3	Communications enable networks and telephone systems to function. Disruption will result in loss of connectivity to schools. The use of cell-based telephones can help to alleviate this but the main reliance is on the land based lines.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY HIGH	1	TERMINAL
2	HIGH	2	DEVASTATING
3	MEDIUM	3	CRITICAL
4	LOW	4	CONTROLLABLE
5	VERY LOW	5	IRRITATING

IS 020105 Serious Information Security Incidents

COMPLETED BY	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
REVIEWED BY	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

The ISCP Project Team has examined each potential disaster or emergency situation resulting from serious information security incidents. The focus here is on the level of business disruption that could arise from each type of disaster.

Potential disasters as a result of serious Information Security incidents have been assessed as follows.

POTENTIAL DISASTER	PROBABILITY RATING (SEE TABLE BELOW)	IMPACT RATING (SEE TABLE BELOW)	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Cyber crime	5	3	Cyber crime is a major area of information security risk. It includes attacks by hackers, denial of service attacks, virus attacks, hoax virus warnings and premeditated internal attacks. Cyber crime attacks can have an immediate and negative effect on normal business processes.
Loss of records or data	5	3	Can be particularly disruptive where poor backup and recovery procedures result in the need to re-input, IF data is available. This is normally a slow process and is labor intensive. Can result in an increase in costs through additional working hours and confusion when information is unexpectedly not available.
Disclosure of sensitive information such as student identification numbers, class file data, special education or medical data, etc.	4	3	A serious information security incident, which can result in severe embarrassment, financial loss, and even litigation. Unauthorized disclosure of certain student information

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

			can be particularly serious, as can financial and strategic plans, personnel issues, etc.
Information Technology failure	4	3	There is almost total dependence on IT systems within our system. A failure to those systems can be particularly serious. The types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air conditioning system failures, network failures, application system failures, telecommunications equipment failures etc.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY HIGH	1	TERMINAL
2	HIGH	2	DEVASTATING
3	MEDIUM	3	CRITICAL
4	LOW	4	CONTROLLABLE
5	VERY LOW	5	IRRITATING

IS 020106 Other Emergency Situations

Other potential emergency situations have been assessed as follows:

POTENTIAL DISASTER	PROBABILITY	IMPACT	BRIEF DESCRIPTION OF
--------------------	-------------	--------	----------------------

COMPLETED BY	NAME:	Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
REVIEWED BY	NAME:	Dr. John Lairsey, Superintendent of Schools	DATE:

	RATING (SEE TABLE BELOW)	RATING (SEE TABLE BELOW)	POTENTIAL CONSEQUENCES
Workplace violence	5	3	Acts of violence in the workplace can affect morale, absenteeism, create fear and uncertainty, and increase the rate of turnover of employees. This can have a significant effect on productivity and could also result in claims for workers compensation, harassment claims, and a need for increased security measures.
Neighborhood hazard	4	5	A neighborhood hazard is defined as a disruptive event in the close vicinity, which directly or indirectly affects our buildings and employees. An example would be a gas leak or sewer main break. Health and safety regulations require that the organization take suitable action to protect its employees. This may have severe implications, particularly where it can take some time to clear the hazard.
Employee morale	5	4	A large number of internal or external factors can have a direct impact on the level of employee morale. This can arise where there is a combination of poor management, uncertainty, and difficult working conditions. Productivity will be affected and employee turnover is likely to rise.
Legal problems	5	4	Legal problems are both time-consuming and expensive. Organizations can experience a wide range of legal issues including sexual harassment, contract disputes, work and wage disputes, health and safety

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

			regulations and discrimination. It is important for us to be fully aware of our legal duties and the rights of our employees.
Negative publicity	4	4	Unfavorable press comments can result in a lowering of employee morale or a loss of confidence by parents and other citizens. Information can be leaked to the press from disgruntled employees and persons who do not understand a situation. We are not exempt from negative publicity and an internal crisis is best resolved from within, prior to the media feeding off the uncertainties and disputes. Reports may also be inaccurate, particularly where reliable information is not available, and therefore, well-worded press statements may be issued to quiet down adverse reports.
PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
1	VERY HIGH	1	TERMINAL
2	HIGH	2	DEVASTATING
3	MEDIUM	3	CRITICAL
4	LOW	4	CONTROLLABLE
5	VERY LOW	5	IRRITATING

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020304 Key IT and Communications Suppliers and Maintenance Engineers

The following contains a list of the key IT, communications suppliers and maintenance engineers, together with their emergency contact information, to ensure that they can quickly be contacted in the event of an emergency.

NAME OF IT SYSTEM	VENDOR/MAINTENANCE SUPPORT FIRM	CONTRACTED MINIMUM RESPONSE TIME	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS
IBM Server (Financial and Personnel) Serial: KQDGGRB Printer: HP LaserJet 4350tn HP Contract 3yr parts only Customer: 1336331	Genesis (Software) GADOE IBM HP	Not contracted Site & Parts - 3yrs Parts only-3yrs	706-654-5470 800-234-1490 x4-1 800-HPINVENT	706-654-5470 800-234-1490 x4-1 800-HPINVENT
Network Systems	Ruckus Wireless HP	Contracted – warranty	855- 478-2587 800-474-6868	855- 478-2587 800-474-6868
Network Communications	AT&T Peachnet Wind Stream	24X7 (GADOE) Internet Service 24X5 Contracted	800-222-8926 706-583-2000 496-7000	800-222-8926 912-282-6452 or 800-501-1776

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020303 Key IT Personnel and Emergency Contact Information

The following is a list of the key IT personnel and emergency contact information to ensure that that the persons responsible for back-up and recovery of specific systems can be quickly contacted in the event of disruption to normal business operations. During an emergency the phone emergency contracted response system, One Call Now, contacts all key employees. Dr. John Lairsey makes the initial call to the service, which then contacts each department head at the board office and school principals. The department heads contact their staff listed below. Each staff member listed below is responsible for their given department and all backed up records or equipment removal from their school or site.

NAME OF IT SYSTEM	NAME OF KEY STAFF	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS
Genesis/Infinite Campus (Finance and Personnel) IT Contacts	Dr. John Lairsey	496-2501 ext 2400	912-276-0673
	Patsy Allen	496-2596 ext 2003	912-496-7230
	Barbara Jones	496-2596 ext 2011	912-496-3602
	Danny McCoy	496-2360 ext 2205	912-390-1069
	Dr. Josh Howard	496-2501 ext 2405	912-276-0672
	Michael Walker	496-7369 ext 2305	912-276-0675
	Dr. Drew Sauls	843-2383 ext 2105	912-614-3949
	Shelia Smith	496-2596 ext 2001	912-276-4125
	Dr. Sandy Slater	496-2596 ext 2010	912-269-4999
	Ryan Relihan (Contracted Engineer)	912.422.4919	912-422-4919
Windows 2008/2012 Server Network	Dr. Sandy Slater (BOE)	496-2596 ext 2010	912-269-4999
	Patsy Allen (BOE)	496-2596 ext 2003	912-496-7230
	Meagan Oakley (CCHS)	496-2965 ext 2410	904-845-7344
	Dr. Sandy Slater (FES)	496-7068 ext 2324	912-496-2301
	Dr. Teresa Bradley (BMS)	496-2360 ext 2203	912-496-7832
	Tommy Harris (SGE)	843-2383 ext 2116	912- 288-7427
	Ryan Relihan/MTC (Contracted Engineer)	478-283-0565 478-954-4012	478-283-0565

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020302 Key IT, Communications and Information Processing Systems

The most critical IT processes and information-processing systems are listed below in order to be able to identify the business processes that will be affected if there is an interruption to the IT system availability.

The organization's key systems are as follows.

SYSTEM	VENDOR/ SUPPORT FIRM	VERSION	PLATFORM/ OPERATING SYSTEM
DELL POWEREDGE (PERSONNEL) & IBM X3500(FINANCE)	IBM & DELL	IBM & DELL (MOST RECENT)	WINDOWS 2008/2012 SERVERS
KEY BUSINESS USERS: Superintendent, Assistant Superintendents, Directors, Coordinators, Principals, and their authorized office staff.			
ALL WINDOWS-BASED SERVERS ON NETWORK	DELL & IBM/LENOVO	VARIOUS (MOST RECENT)	WINDOWS 2008/2012 SERVERS
KEY BUSINESS USERS: All staff uses email, calendars, and other common applications. Many key staff uses the Student Information System, timekeeping, etc.			
KEY BUSINESS USERS:			
KEY BUSINESS USERS:			

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020305 Existing IT Recovery Procedures

A summary of the existing IT back-up and recovery procedures are documented below, covering both hardware and software systems, data backup and recovery processes. This includes any off-site data storage arrangements.

Networked Systems

Windows 2008/2012 servers (eMail, SIS, Internet, etc.)

Recovery procedures were implemented and tested at system installation for all servers. A full backup of the servers at each school is performed one day of the week and incremental or differential backup the other week days. All backup files are backed up to an off location Teradrive over the weekend by contracted engineer, Ryan Relihan.

All email is backed up through Google in the Gmail Vault program. The email server is located in United States, with backups of all emails through Google Email Vault services.

GENESIS/Infinite Campus (Financial and Personnel System)

Recovery procedures were implemented and tested at system installation for all servers. A full backup is performed each night. We utilize two sets of tapes/CDs, one for daily backups, and another for weekly backups. Weekly backups use a set of 7 tapes/CDs. Every Monday morning, the backup tape from the preceding Friday is removed to off-site storage, a fire-proof safe off location. Finance persons will maintain backup files at the board office for Genesis system. Technology Director will maintain backup files and Teradrives for all other system records. Contracted engineer, Ryan Relihan, Network Engineer Services, completes all system server backups and recovery off location. Cloud backups are maintained for all backups and for the school district program Infinite Campus. Written agreement attached.

Direct Deposit/Payroll checks printing: All files are backed up to a Teradrive, which will be moved from the board office with the Finance person during any emergency. The computer, check printer & signature card will be removed with backup records by the finance person or technology director (if not available) to a location off the campus.

All necessary equipment will be moved by Finance person or Technology Director to a school vault, if available or to a government facility (OERC or County/City building) until the emergency is over, as determined by the emergency situation. If a fire, then and only if they can remove the equipment safely moved to a school location or government facility. Hurricane, etc. will move to a school vault or government facility.

<i>COMPLETED BY</i>	NAME:	Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME:	Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020403 External Emergency Services and Contact Numbers

Contact numbers for public emergency services and other commercial emergency service providers are listed below.

EMERGENCY SERVICE	CONTACT NUMBER	CONTACT NAME
Fire, Police, EMS	911	Charlton EMS
Transportation and Maintenance	496-7226 Use radio/cell phone in emergency	Charlton County Schools Ralph Bartram/Jeff Highsmith
Georgia Natural Gas Company	800-427-5463	800-427-5463
Georgia Power	888-660-5890	24-hr Service Line or 888-891-0938
Police Non-Emergency	496-2281	Charlton Sheriff
Animal Control	496-2281	Charlton Sheriff
Charlton County Technology Department Technology Backups Files Off location Network Technology Consulting	912-269-4999/496-2596 ext 2010 478.283.0565/478.954.4012	Dr. Sandy Slater, Technology Director Ryan Relihan, Engineer

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

IS 020502 Back-up Power Arrangements

Back-up generators have been provided in critical areas to allow critical business processes to continue when there is a power outage. UPS systems are used for key equipment or services, which may be affected by sudden surges of power, or where data may be corrupted when the system switches over from mains power to a back-up generator.

Existing back-up power arrangements are listed below, together with the critical functions, which they support:

TYPE OF BACK-UP GENERATOR	CRITICAL FUNCTIONS SUPPORTED	REQUIRED FREQUENCY OF TESTING	DATE TEST LAST CARRIED OUT	PERSON RESPONSIBLE FOR TESTING/ MAINTENANCE
UPS (Various units)	All network file servers, switches, and data and application servers.	Monthly	3-6-16	Dr. Sandy Slater (BOE& FES) Meagan Oakley (CCHS) Dr. Teresa Bradley (BMS) Tommy Harris (SGE)

<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

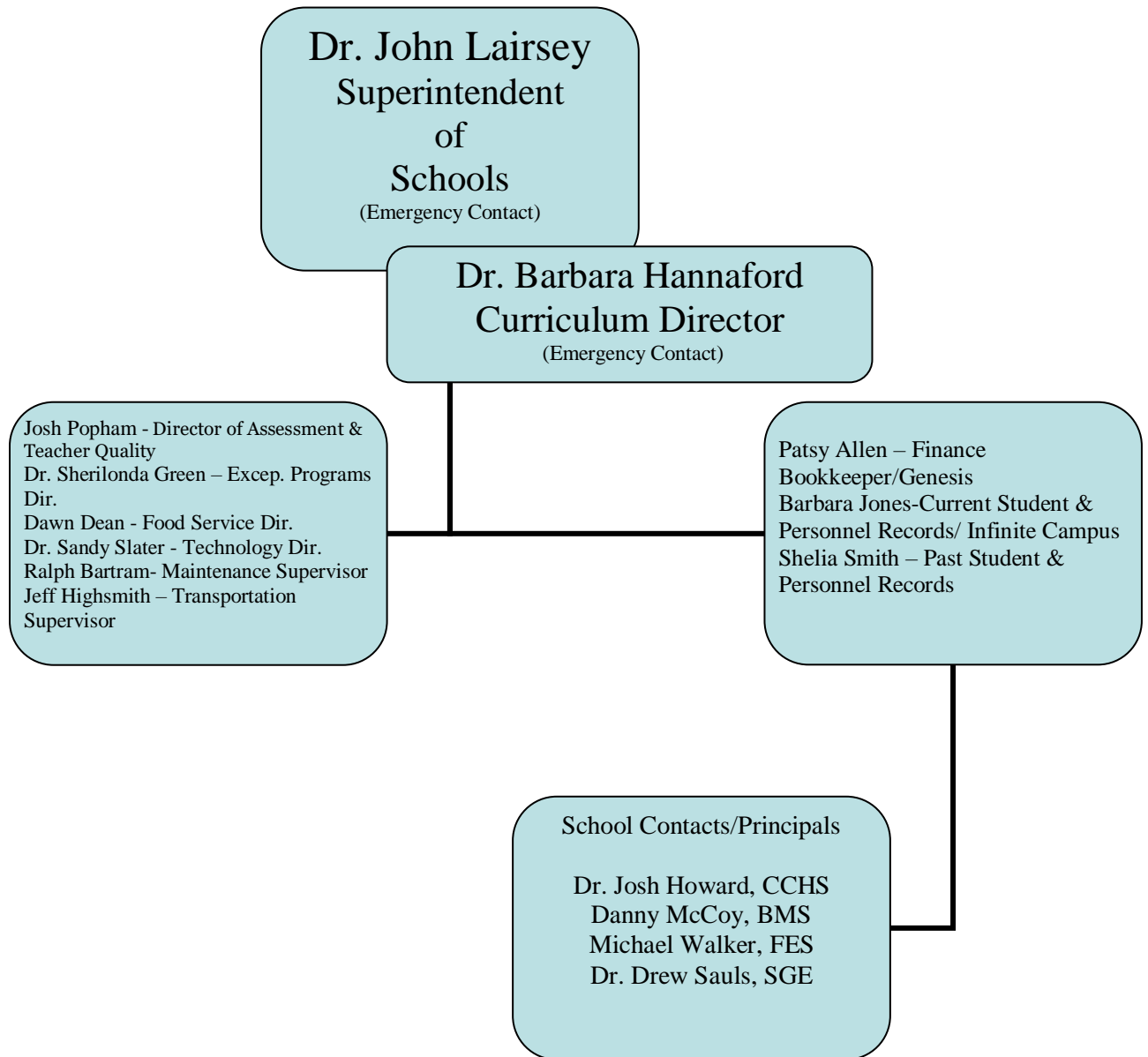
IS 030201 Functional Organization Chart

A list of the organization's key managers and staff, together with a chart showing the functional structure of the organization, are shown below. This information will allow identification of responsibilities and dependencies in the early stages of an emergency. During an emergency the contracted phone emergency response system, One Call Now, contacts all key employees. Dr. Lairsey designated to initiate the emergency phone system calls.

NAME	JOB TITLE	DEPARTMENT OR UNIT
*Dr. John Lairsey	Superintendent of Schools	Charlton County Schools
*Dr. Barbara Hannaford Josh Popham Patsy Allen Barbara Jones Sheila Smith Dawn Dean Dr. Sherilonda Green	Curriculum Director Director of Assessment & Teacher Quality Finance Bookkeeper Student & Personnel Information Records Administrator Past Student & Personnel Records Food Service Director Except. Programs Director	Operations Lead for Emergency Response System Finance Student & Personal Records Past Student & Personnel Records Food Services Except. Programs
Dr. Sandy Slater Ryan Relihan Teresa Bradley	IT/IS Director Network Engineer Lead Media Specialist	IS and Technology IS and Technology IS and Technology
Ralph Bartram Jeff Highsmith	Supervisor, Maintenance Supervisor, Transportation	Maintenance Transportation

COMPLETED BY	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
REVIEWED BY	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:

The chart showing the functional structure of the recovery portion of the organization is as follows:



<i>COMPLETED BY</i>	NAME: Dr. Sandy Slater, Technology Director	DATE: 2-14-2006 Updated: 7-17-2018
<i>REVIEWED BY</i>	NAME: Dr. John Lairsey, Superintendent of Schools	DATE:
