CRITICAL INCIDENT PLAN

Compliance statement

Every policy is reviewed at regular intervals and where applicable, as stipulated by law. Each policy is also available in additional formats including Braille and in additional languages upon request, within reasonable timescales as stipulated by the school.

Reviewer/s:	Danielle Ashley
Last reviewed on:	November 2023
Next review due by:	December 2024
Approved by:	Full Governing Board

‘Together we can, with Christ by our Side.’

CONTENTS

List of Annexes

Annex G Emergency Response Plan: Training, Exercise and Maintenance Record Sheet

Distribution List

(Name of plan recipients, organisation and number of copies distributed to each)

Headteacher
SBM
DHT
AHT
Office (Infant)
Office (Junior)
Caretaker's Office

Chair of Governors (Off -site Copy)

Presbytery – Virgo Fidelis Church (Off-site Copy)

<u>Note</u>: A copy of this plan should be kept off-site by a nominated person in case access to computers and/or the school building, where the details are normally, kept is denied.

1:0 General Information

Name:	The Federation of St Joseph's Catholic Junior, Infant and Nursery Schools
Address:	Infant & Nursery – Crown Dale, SE19 3NX Junior – Woodend, SE19 3NU
Telephone Number:	Infant – 0208 670 2385 Junior – 0208 653 7195
Headteacher:	Mrs Danielle Ashley
Type of School:	Voluntary Aided
Pupils:	Mixed
No: of Pupils:	Infant – 140 + 30 nursery children Junior – 208
Age range of pupils:	4-11

Operating Hours: **Core School Hours**:

Playground Supervision (Starts)	Start of morning session	Morning Break	Lunch Time	Start of afternoon session	End of School
Junior 08:40hrs Infant 08:45hrs	08:50hrs 0850hrs	KS1- 10:30 KS2 – 10.30	KS1 1215 noon KS2 1215 noon	KS1 1315hrs KS2 1315hrs	KS1 1510hrs KS2 1515hrs

Extended School Activities:
Details of any extended school activities operated by the school for pupils, including type of activity, days and times. **(see Annex) All after school clubs finish by 16.15hrs**

External Clubs (see 4:0 for contact details)
Details of any external clubs that hire the school facilities. Including type of activity, days & times
Breakfast Club (Garden Hall) – daily from 0730hrs*
After School (Garden Hall) – daily to 1800hrs*
*run by Mrs Stephanie Odewale

Special Notes: School Nursery on site, Full day, am and pm sessions. Max 30 pupils per session.

Keyholders: See 4.0, SERT contact details for keyholders.

Rest Centre: The School **is not** a designated rest centre.

School Term Dates: The School term dates for 2022/2023 are detailed at Annex A *(This page will be updated each year with the new annual term dates).*

2:0 Risk Assessments

2.1 School Outings and Activities

In accordance with Croydon Council's 'Educational Visits and Journeys: Guidance for Organisers' The Federation of St Joseph's Catholic Junior, Infant and Nursery Schools undertake risk assessments for all school trips and activities that it participates in.

The risk assessments/EV forms are located in the *admin office on both sites*

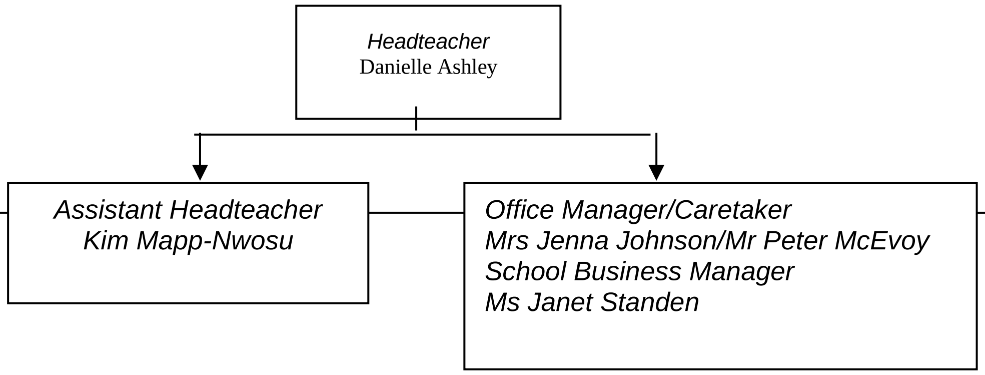
Current trip forms are located in the school office.

2.2 Other Hazards

Example: The following chemicals are held in *(location):*

Chemical	Notes
Bleach/cleaning fluid	In cleaning cupboards of both sites (min stock held) or metal cabinet in kitchen area

Emergency Response Team Structure



Headteacher
Danielle Ashley

Assistant Headteacher
Kim Mapp-Nwosu

Office Manager/Caretaker
Mrs Jenna Johnson/Mr Peter McEvoy
School Business Manager
Ms Janet Standen

Annex C: SERT Action Sheets, lists suggested tasks that need to be undertaken by the above roles in the response to an incident. Tasks may well be interchangeable depending upon the availability of resources and other commitments in an emergency.

3:2 Control Centre Details

List the designated area from which you will co-ordinate the school's management of an incident. For example:

	Designated Location
Control Centre	Head Teacher’s Office
Reserve	ICT Suite (Infant & Junior Schools)
Off-site Reserve	Presbytery, 143 Central Hill SE19 1RT (020 8670 2777)

See **Annex B** for school site plan

3:3 Emergency Expenditure

In an emergency situation, the Chair of Governors has delegated powers to make an urgent decision about the allocation of resources from within the School’s delegated budget as long as this is reported to other governors in due course.

Any request for the allocation of additional resources outside of the School’s delegated budget will need to be channelled through Director of Education Croydon and Director of Commission for Schools and College (Archdiocese of Southwark).

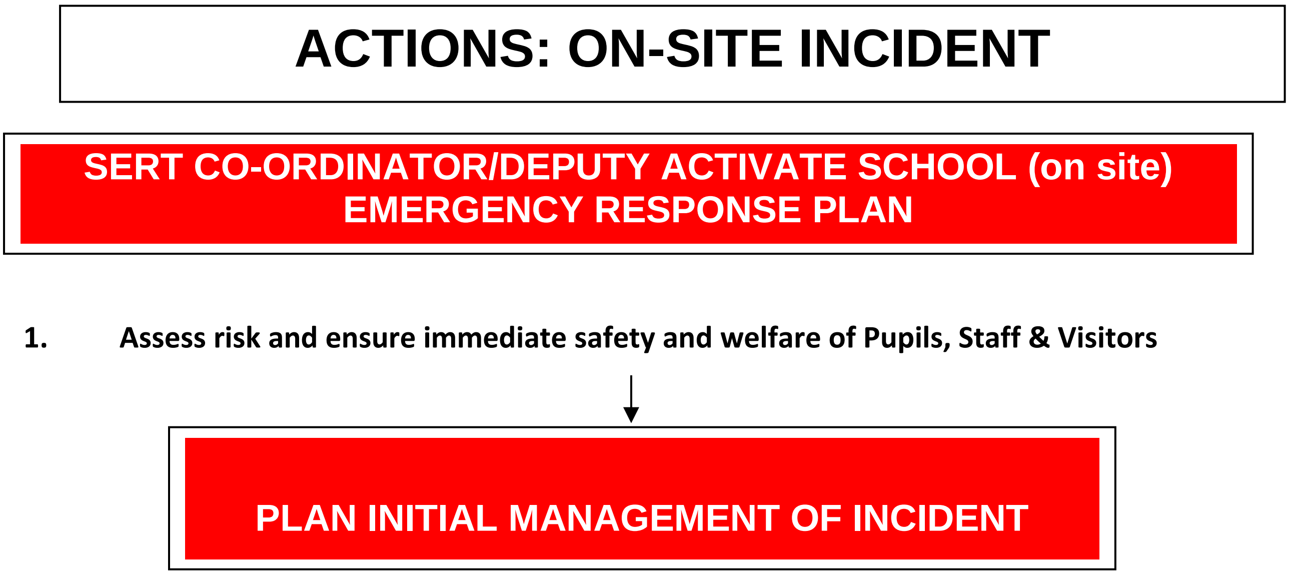
3:4 Generic Response to on-site/off-site incidents

Flexible procedures need to be developed to ensure that an efficient response to a crisis can be achieved. The procedures detailed in Fig. 1 & 2 (overleaf) are not exhaustive; the type of response will largely depend upon the incident but they outline the main actions that need to be taken into consideration.

3.5 Training & Exercising

Training staff and exercising the response procedures detailed in your emergency plan are integral parts of the emergency planning process. See **Annex G**:

Figure 1



ACTIONS: ON-SITE INCIDENT

SERT CO-ORDINATOR/DEPUTY ACTIVATE SCHOOL (on site) EMERGENCY RESPONSE PLAN

1. **Assess risk and ensure immediate safety and welfare of Pupils, Staff & Visitors**

PLAN INITIAL MANAGEMENT OF INCIDENT

♦Dealing with Enquiries
♦Informing Families of those Involved
♦Transport
♦Resources/Materials
♦Communication
♦Re-uniting Pupil with Parent/Guardian

♦Media
♦Access Control (Police)
♦Special Needs
♦Cultural/Religious Issues
♦Mutual Aid
♦Business Continuity Management

PLAN LONG-TERM MANAGEMENT OF INCIDENT

♦Security of Site/Preservation of evidence
♦Clear up of Affected Area of School
♦Support for Pupils/Staff/Families
♦Acknowledgement of Incident
♦Gifts/Cards to Injured Persons
♦Planning Memorials & Commemorations
♦Restoring normality
♦Public Inquiry/Investigation/Legal Implications

♦Media
♦Business Continuity Management
♦Reputation
♦Attending Funerals
♦Discussion Opportunities
♦Monitoring the Effects
♦De-briefing & Updating Plans
♦ Financial Implications

Figure 2

ACTIONS: OFF-SITE INCIDENT

SERT CO-ORDINATOR/DEPUTY ACTIVATE SCHOOL (off site) EMERGENCY RESPONSE PLAN

1. **Brief Schools Emergency Response Team (SERT) and mobilise if required.**
2. **Contact Croydon Council/Schools Commission as appropriate**
3. **Contact Parents/Families of individuals involved in the incident**
4. **Brief Staff, Governors, pupils (assembly/class), parents etc… (siblings/close friends should be informed separately)**
5. **Contact any other relevant agencies.**

PLAN INITIAL MANAGEMENT OF INCIDENT

- Dealing with enquiries
- Transport arrangements
- Resources/Materials
- Maintaining normality within the school
- Business Continuity Management
- Reuniting Pupil with Parent(s)/Guardian(s)
- Keeping families informed of information/arrangements
- Advising colleagues at other schools attended by siblings
- Media
- Special Needs
- Communication

PLAN LONG-TERM MANAGEMENT OF INCIDENT

- Business Continuity Management
- Support for Pupils/Staff/Families
- Acknowledgement of incident
- Gifts/Cards to persons injured
- Planning Memorials & Commemorations
- Public inquiry/Investigations/Legal implications
- De-briefing & updating plans
- Media
- Reputation
- Attending funerals/Repatriation
- Discussion opportunities
- Restoring normality
- Financial implications

4.0 Contact Numbers

4:1 The Federation of St Joseph's Catholic Junior, Infant & Nursery Schools contact numbers

SCHOOL EMERGENCY RESPONSE TEAM (SERT)		
Note: List who of the contacts are key holders for the school		
Danielle Ashley **(Key holder)**	**Headteacher**	Work: 0208 653 7195 Work: 0208 670 2385
Mrs Kim Mapp- Nwosu	**Assistant Headteacher**	Work: 0208 653 7195 Work: 0208 670 2385
Mr Peter) McEvoy **(Key holder**	**Caretaker**	Work: 0208 653 7195 Mobile:07949394537
Other School Building(s) Contact Numbers		
Nursery		205#
Garden Hall		312
Emergency Closure Line		
Emergency Closure Line	Croydon Council	0208 726 6400
Governing Body		
Chair	Gillian Murray-Powell	Work: 0208 653 7195 Work: 0208 670 2385
Vice Chairs	Grainne Grabowski Robert Teague	Work: 0208 653 7195 Work: 0208 670 2385
Medical		
School Nurse	Norbury Health Centre (North Croydon) Woodside Health Centre (North Croydon)	020 8679 1700 020 8656 0213
School Educational Psychologist	Dr Nora Dwyer	Octavo
Other School Contacts…		
External Clubs (who hire the facilities)		
Fascinating Rhythm	Mrs Mcmillan	07787518709

Breakfast Club/after school club	Mrs Odewale	07771904069
Training & Behaviour (Puppy Training)	Ms Louise Taylor	07703790825
Archdiocese of Southwark & Parishes		
Commission for Schools and Colleges	Mr Simon Hughes	Tel. 01689 829331 Fax. 01689 829255
Virgo Fidelis	Fr James Clark	Tel: 020 8670 2777 Fax: 020 8670 7578
St Matthew’s	TBC	Tel: 020 8670 1765 Fax: 020 8670 6230
St Margaret Clitherow	Fr Luke Marappillil	Tel: 020 8670 5814
EMERGENCY SERVICES 999		

4:2 Croydon Council / Schools Commission

Croydon	Tel: 020 8726 6400
Schools Commission	Tel: 01689 829331 Fax. 01689 829255
LA Croydon	020 8726 6000
Octavo Partnership	020 8241 5400

THE FEDERATION OF ST JOSEPH’S CATHOLIC JUNIOR, INFANT & NURSERY SCHOOLS

COMPUTER DISASTER RECOVERY AND SECURITY PLAN

Authorised access to FINANCE AND FACILITY:

Headteacher: - Danielle Ashley
School Business :Manager (I/J) Janet Standen
Office Manager : Marzena Johnson

ICT Leader Ms Caron Allery

Deputy DSL Mrs Fiona Langford-Jackson

AHT Kim Mapp-Nwosu

Access to the administration system is limited to known individuals via passwords. Only the above-authorised personnel have access to children's and parents' data.
Please note the Data Protection Act allows disclosure of personal information to other bodies such as the Local Education Authority, Schools Commission etc. Care should be taken when disclosing personal information.

The school is registered under the current Data Protection Act

All data for management purposes, e.g. Facility is backed up nightly by SIMS and Network Server.

ntivirus software (Sophos) is installed on all computers and is regularly updated through Openair.

Curriculum Network

The ICT Leader ensures that pupils save their work to the network or online space in Purple Mash and not to USB drives. Students work is backed up overnight to enable recovery in the event of the loss of data files or system failure. Back up is undertaken by Gridstore through Openair. The back-up log on the server is checked regularly to ensure that the back-up has been carried out successfully.

Management hardware and the server system network is covered by a maintenance contract with Openair (Gridstore). Therefore server operating systems and drivers will be reinstated by them and all software and hardware will be replaced and re-loaded in the event of failure, theft, etc.

The school has Virus protection installed (Sophos) on all computers including the server. The virus protection is regularly updated and all staff are aware of the importance of allowing the updates to proceed. If a virus is identified by a computer then this is reported immediately to the ICT Leader who will take action to ensure removal of the virus. The infected computer should not be used until the virus has been removed and should be removed from the network.

All staff are aware of the Internet Use and E-mail regulations and Acceptable Use Policy. They have all signed an acceptable use agreement.

For Insurance Purposes

All computers, printers, equipment etc. are listed on the School Asset system with serial numbers and other relevant information. These inventories are maintained regularly by the School Business Manager and ICT Leader. Software licences are listed and maintained by the ICT leader. The insurance company is kept informed of acquisitions of new equipment (as dictated by the policy covering the school).

The ICT Leader together with the Headteacher are responsible for carrying out the disaster recovery plan. A copy of this plan is kept off-site.

In the event of a disaster staff, pupils and support services are kept informed of the situation.

The disaster recovery plan is tested and updated regularly.

Staff are aware of the existence of the Disaster Recovery Plan.

In the Event of a Major Disaster:

An outline recovery plan will need to be prepared and actions prioritised. An event log will be started and maintained and all key events will be recorded. Any follow-up action will also be recorded. The disaster recovery plan should be reviewed as a result of this log.

The primary objective of this IT Disaster Recovery Plan is to help ensure continuity of service for the Federation by providing the ability to successfully recover computer services/data in the event of a disaster.
Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster,
- Minimising confusion, errors, and expense to the school, and
- Implementing a quick and complete recovery of services.

ROLES
The following Roles have been identified and they report to the Headteacher (or Senior Management Nominee):

- ICT Leader in liaison with School Office Managers

The following Roles have been identified and report (on a technical basis) to School Business Manager, ICT Leader & Office Managers

- **Openair** as a support based service on which the schools depend (network, security, firewall, email, SPAM, content filtering, remote backup, etc). This is a bought in service – SLA renewable annually.

SCOPE
This plan will only address the recovery of systems under the direct control of the School and assumes (rightly or wrongly) that the services “bought in” from Openair and other providers, have their own IT Disaster Recovery and Business Continuity Plans in place for the services that they provide. In reality, this is a pragmatic assumption short of the school committing to the expense of dual sourcing these components.
Also, given the uncertain impact of a given incident or disaster, it is not the intention of this document to provide specific recovery instructions for every system. Rather, this document will outline a general recovery process which will lead to development of specific responses

to any given incident or disaster.

IT Disaster Recovery Action Plan

This plan recognises that its implementation cannot happen over night and that the school, Governing Body, Openair, Octavo and 3rd party suppliers will need to work over time to make this plan a reality. In the interim backup regimes for critical files/data, etc. already in operation should continue "as is" until the Headteacher specifically indicates those activities are redundant.

ASSUMPTIONS

This disaster recovery plan is based on the following assumptions:

- Once an incident covered by this plan has been declared a **disaster**, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.
- Depending on the severity of the disaster, all users of IT may be required to modify their operations to accommodate changes in system performance, computer availability and physical location until a full recovery has been completed.
- 3rd party bought in services (such as LGfL systems, the internet broadband, service etc.) come with adequate protection against malicious software, viruses, trojans and security compromise at source rather than the School having to specifically protect each individual computing resource.
- No 3rd party computing devices (personal laptops, mobile computing devices, etc) are allowed to gain access to the school network (physical or wireless) or gain any form of peer to peer network connection, unless specifically audited and authorised.

DEFINITIONS

The following definitions pertain to their use in this IT Disaster Recovery Plan:

- **Backup/Recovery Data**: Copies of all software and data deemed critical or valuable. This data will originate on the central server. The backup and recovery data will exist in separate file systems and may be held locally and remotely to the school. The backup data is used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.
- **Disaster**: A significant or unusual incident that has long-term implications to the working of the school whereby the maximum tolerable outage (MTO) has or will have been exceeded.
- **Incident**: An event which impacts a specific IT service, server or data.
- **Level 1 Risk**: Risk associated with the loss of the **most** critical IT services, capabilities, applications or data.
- **Level 2 Risk**: Risk associated with the loss of or impairment to critical IT services, capabilities, applications or data.
- **Level 3 Risk**: Risk associated with the loss of other identified IT services, capabilities, applications or data.

RESPONSIBILITIES

The **Headteacher** is responsible for:

- **Management of this plan**

And in particular management of the ICT Leader & Office Managers and School Business Manager.

- **IT Contacts Register**

The school will maintain a contact list for all suppliers (hardware, software, service, advisors, insurers) that have an impact on this plan. This should also seek to encompass similar institutions that have agreed to provide reciprocal shared services to the school in an emergency.

- **Establishing SLA's**

Suppliers of hardware, software and particularly service elements of this plan need to be able to commit to responding in timeframes that allow the school to meet the defined MTO's. Where possible this should be written into their existing service level agreements or contracts with the school.

The **ICT Leader, School Business Manager and Office Manger** are responsible for (but do not necessarily undertake personally):

- **System Audit**

Definition and documentation of all key components on the system (including information for insurers), upgrade status, the licence information, network shares, (whether standard or custom built), basic hardware level, file system types.

- **System Build/Restoration**

Restoring from image or re-install disks, upgrading to latest software levels, restoring users, restoring networking & network access, restoring file access & privileges.

- **System Maintenance**

Keeping software revisions up to date as per software providers' recommendations, upgrading the OS with latest patches/service packs, registry cleaning, file system integrity checking/defragmenting.

- **System Security**

Maintaining virus protection, email scanning, personal firewall (for mobile devices), phishing, spyware & intrusion protection, user access rights & privileges, system password rotation, user password strength & regime, wi-fi lockdown.

- **Data Access Control**

Setting up user based roles and access to appropriate data and maintaining those rights on any utilised backup devices.

- **Backup/Restore**

Ensuring the central server has hardware RAID protection against individual disk failure. Local backups to be conducted to external network attached storage device. Setting up and monitoring success of full and incremental backup regimes for all critical & valuable data secured on the central server. Copies of master software disks should be made (usually allowable as part of the licence agreement) and stored off school premises.

- **Local DR Testing**

Undertake a once a year local DR test in isolation of the school critical incident plan that encompasses a system build and restoration of "lost data". Actual and successful occurrences of such a task performed in the normal course of events (when adequately documented) to count towards this exercise.

- **Plan Update**

The output of the DR testing (live or simulated) should be used as a trigger to validate and adjust this plan on an ad hoc basis as should the introduction of significantly new or different IT systems to the school. Outside of these triggers, this plan should be reviewed annually.

GENERAL DISASTER RESPONSE & RECOVERY GUIDELINES

Data that is deemed critical or valuable will be held on the school's network to facilitate regular centralised backup and management of systems.
Data access to the centralised server is done by standardised named "shares" and access rights to sensitive data controlled by user based privileges.
No critical or valuable data will be held on local computing devices unless local backup arrangement is in place & functional (memory sticks, local external disks, etc.) and authorised by the school. This backup data is to be held separately & securely from the original source.
Wherever possible (and where licensing permits) computers of similar function should be of a standard & documented build allowing fast rebuild from a system image. Rebuild or upgrade of these systems should be regular to maintain the operating system and key software components to the provider's specification.
In the event of a non-obvious disaster, the Headteacher will be notified.
The Headteacher will identify individuals required to assist in the recovery process.
The school will be informed as to IT system degradation and restrictions on IT usage and/or availability.
These designated individuals will develop an overall IT recovery plan and schedule, focusing on the School's highest priorities as defined by the component **Risk Level.**
Necessary software and hardware replacement will be coordinated with vendors and the School's insurer.
The recovery status updates will be communicated to the Headteacher.
The Headteacher will verify restoration of the IT infrastructure to pre-disaster functionality.

IT RISK ASSESSMENT

For each main area of IT usage (Computer Suites, Administration PCs/Servers, Headteacher's PC, SLT PC, Classroom PC, School Laptops, Offsite backup systems), IT Risk assessments will be performed by the Subject Leader & Headteacher covering:

- **General**

Description of the IT in place (PCs, printers, scanners, networking, storage) its function(s), users, capability, use for private/sensitive/controlled data.

- **Physical/Security Risks**

Access doors, windows, public/private space, lockable room, alarms, security cables, video surveillance.

- **Environmental Risk**

Flooding (flat roof, ground floor plumbing, fire system), fire, extreme temperatures (inc a/c)

- **Internal Systems Risk**

Networking infrastructure, cabling

- **External Systems Risk**

Power, BT communications, Internet Service provision, quality of software updates

- **Recovery Planning**

Alternate space, systems, service provision, shared services available

- **Risk Assessment Level**

Level 1, 2 or 3

- **MTO Definition**

The time at which the loss of this service, facility or data would be declared outside the scope of normal expected and planned for acceptable failure and be considered a "disaster" that warranted immediate attention.

- **Estimated time to procure replacement**

Hardware (and or software if media destroyed).

- **Estimated time to recover to new hardware**

Rebuild of systems from scratch or from system images and re-establishment of data, links to data and other services

- **Requirement for Resiliency/Back-up**

None
Hardware RAID storage system
Backup – local, offsite, both
Backup regime – Full/Incremental
Data Sensitivity – User Access Control or Encryption.

- **Preventative & further measures required**

Identify **measured and proportionate** improvements to current facilities which will serve to reduce risks. Suggest a timescale for agreement and implementation so that items can be prioritised correctly While it may be that having conducted risk assessments, it is determined that the loss of much of the IT infrastructure individually (classroom PC) or in larger groups (library) would have only minor impact to the teaching or management of the school, it will at least serve to highlight those **key** components which should be the subject of the higher priority activities for prevention and for DR testing.

Finance Documentation:

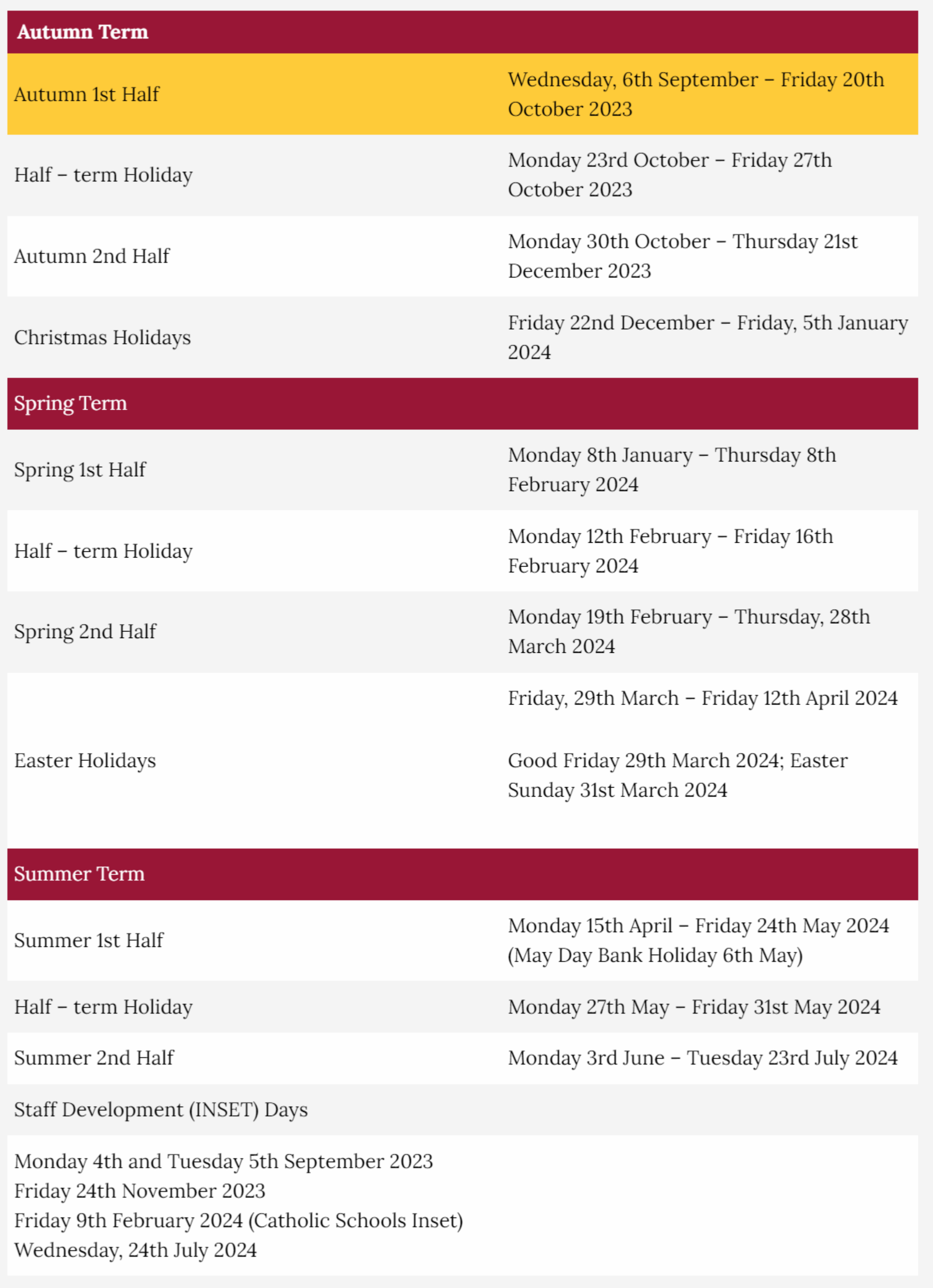
The following items will be kept in the safe in order to maintain usage after a fire/flood damage etc.

- Cheque books
- School Fund
- Bank Mandate

All transactions, orders etc are put onto SIMS and are therefore available through Fronter off site if required.

Annexes

Annex A	**School Term Dates**
Annex B	**Site Plans**
B-1	**School Site Plan**
B-2	**Location Map (Showing emergency services access route)**
Annex C	**SERT Action Sheets**
C-1	**Co-ordinator**



Autumn Term	
Autumn 1st Half	Wednesday, 6th September – Friday 20th October 2023
Half – term Holiday	Monday 23rd October – Friday 27th October 2023
Autumn 2nd Half	Monday 30th October – Thursday 21st December 2023
Christmas Holidays	Friday 22nd December – Friday, 5th January 2024
Spring Term	
Spring 1st Half	Monday 8th January – Thursday 8th February 2024
Half – term Holiday	Monday 12th February – Friday 16th February 2024
Spring 2nd Half	Monday 19th February – Thursday, 28th March 2024
Easter Holidays	Friday, 29th March – Friday 12th April 2024 Good Friday 29th March 2024; Easter Sunday 31st March 2024
Summer Term	
Summer 1st Half	Monday 15th April – Friday 24th May 2024 (May Day Bank Holiday 6th May)
Half – term Holiday	Monday 27th May – Friday 31st May 2024
Summer 2nd Half	Monday 3rd June – Tuesday 23rd July 2024
Staff Development (INSET) Days	
Monday 4th and Tuesday 5th September 2023 Friday 24th November 2023 Friday 9th February 2024 (Catholic Schools Inset) Wednesday, 24th July 2024	