

IT Business Continuity Plan

Definition of IT Business Continuity Management

IT Business Continuity Management is defined as a holistic management process that identifies potential impacts that threaten the IT systems, processes and data of The Education Fellowship and provides a framework for building resilience with the capability for an effective response that safeguards the interest of its key stakeholders, reputation and value creating activities.

These impacts or 'crisis' include:

- 🛡️ Building or site incidents: for example, flood, fire, terrorist attack on buildings affecting access to or from buildings and sites
- 🛡️ Infrastructure incidents: for example, loss of computer / telephony systems, loss of power
- 🛡️ Staff / Operational incidents: for example, loss of key staff, loss of critical systems
- 🛡️ Widespread environmental factors: for example, flu pandemic, fuel shortages

The Education Fellowship IT Business Continuity Plan consists of one plan to cover different IT operations, based at Fellowship House. Separates plans will be incorporated for operations based at The Education Fellowship schools. The primary objective of the Business Continuity Plan is to show how The Education Fellowship would respond to identified risks and continue to manage its operations under adverse circumstances.

Crisis Management Group

If a major disaster occurs then The Education Fellowship Crisis Management Group will be mobilised. The membership of this group will be all members of The Education Fellowship Executive. All communication with the media must be via The Chief Executive's Office

Documentation and location (example below)

Name of document	Location
Business Continuity Plan Appendix A: Crisis Management Group Appendix B: Key Stakeholders Contacts Appendix C: Staff Contact Details Appendix D: Organisational Chart	Staff Notice Board Reception Human Resources Department Staff Handbook

Review of Business Continuity Plan

A comprehensive review of risk is taken at least annually by The Education Fellowship Executive. These revised plans must be submitted to the CEO for incorporation within The Education Fellowship Business Continuity Plan.

The different response elements of the plan should be tested.

Training

All staff are made aware of their roles and responsibilities as part of their induction, supervision and performance review. Their responsibilities include awareness of key policies and procedures, including the Business Continuity Plan. Staff must take personal responsibility to ensure they are familiar with the content of the Plan so they know who to contact in case of an incident and how they can contribute to the plan's implementation.

Coordinated Responses

The Plan should not be implemented in isolation, but where possible, should be used in conjunction the Business Continuity and Emergency Plans of the host local authority and emergency services in which it operates.

Risk Assessment and Response

The following table identifies some of the main risks, their likely level of impact on operations and the planned responses to address these risks.

Risk Area	Details	Risk Level	Action / Response
Fire	Caused by carelessness, accident, terrorism, etc.	Low	The School Improvement Officer has overall responsibility in respect of health and safety risks In accordance with the Fire Precautions (Places of Work) Regulations 1997, there are Emergency Planning Procedures in place.
Loss of data	Caused by technical fault, human error or sabotage	Medium	All electronic files are backed up every night stored on Office 365 cloud services Key paper documents are scanned and held electronically
Electrical Failure	Loss of electrical power to Fellowship House	Medium	All systems and data can be accessed remotely through Office 365 cloud services
Theft	Theft of IT equipment	Medium	All systems and data are protected by 128-bit encryption (minimum)
Natural Disasters	Destruction or disablement of Fellowship House	Low	All systems and data can be accessed remotely through Office 365 cloud services
Loss of Human Resource	Death or Disablement of key personnel	Low	All systems and data can be restored or accessed remotely by key staff

Recording Incidents

Details of major incidents and action taken will be recorded. These notes may be referred to if there is any further investigation and it will also inform future business continuity planning.

Key Contacts

Head Office	01832 770515
-------------	--------------

Crisis Management Concerns

Step One

If you have a concern, the first point of contact should be your **line manager**. This can be done orally or in writing.

Step Two

If you feel unable to raise the matter with your line manager, for whatever reason, please raise the matter with a member of The

Step Three

If step one and two have been followed and you still have concerns, or if you feel the matter is serious and cannot be discussed with any of the above, you should contact the Chairman of the Board of Trustees.

Handling the Matter

Once we know of your concern, we will look into it to assess initially what action should be taken. This may involve an internal enquiry or a more formal investigation. We will tell you who is handling the matter, how you can contact them and whether any further assistance may be needed. You can request a written summary of your concern/s and how the organisation proposes to hand it/them. If your concerns fall more properly within the grievance procedure, we will tell you.

In the case of a situation under the Safeguarding (Adults / Children) policy, the concern will be handed across to the relevant Statutory Service to investigate.

If you feel that the matter has not been dealt with in accordance with the law, there are other organisations you can contact depending on your concern.