University
Critical Incident Management Plan

July 2018
Foreword

This Critical Incident Management Plan (CIMP) is designed to ensure that the University has in place management structures, and in particular communication lines, to enable it to respond appropriately to any critical incident, and that it has ready access to the information it might need to respond quickly and effectively to any such incident.

It does not purport to prescribe precisely how faculties, schools, services, or the University centrally should respond to all possible types of ‘critical incident’. Nor does it purport to constitute a detailed ‘disaster recovery’ (or ‘business continuity’) plan.

A ‘critical incident’ may be defined as any event which threatens severely to disrupt, in whole or in part, the functioning of the University, a faculty, school, or service, or which carries the risk of significant adverse publicity (or both). This definition is inevitably vague and it is probably impossible to identify in advance all types of event which would constitute a critical incident. But a critical incident could occur at any time and, regardless of its precise character, would require an organised management response which is prompt, clear and effective. This plan is intended to facilitate that kind of response.

The plan is divided into three parts, as follows.

- **Part 1** provides an overview of the CIMP, and reviews the circumstances in which it might be appropriate formally to activate the plan through either a Gold, Silver or Bronze command.
- **Part 2** outlines critical incident management structures and communication lines at the **CORPORATE** level – the ‘Gold Command’. In particular, it gives the composition of the Critical Incident Management Team (CIMT); sets out arrangements for the establishment of a major incident control centre; and enunciates guidance on communication lines.
- **Parts 3 and 4** are aimed at faculties, schools and services. It summarises the responsibilities of **LOCAL** managers, and the establishment of Silver and Bronze commands.

Further information is provided in annexes, as follows.

- **Annex 1** provides contact details for members of the CIMT and other key individuals.
- **Annex 2** lists the faculties, schools and services that make up the University. It is this list which forms the basis of the cascade system of communication which would be used in the event of a critical incident.
Part 1: Overview

This section gives an overview of the CIMP and reviews the circumstances in which it might be appropriate to activate Gold, Silver or Bronze command.

Activation of the CIMP at Gold Command

1. As is noted in the Foreword, whilst it is perhaps impossible to identify in advance all types of critical incident, such events will usually threaten severely to disrupt, in whole or in part, the functioning of the University, or carry the risk of significant adverse publicity (or both). A critical incident is normally characterised by the following features:
   - there are substantial threats to the safety of individuals or the fabric or reputation of the institution; and
   - it is likely to lead to the suspension of normal operations

   and it follows that a critical incident is likely to require:
   - an organised management response
   - special communications mechanisms
   - the calling out of the emergency services

   and that media interest is likely to be high.

   Examples of critical incidents which are likely to require institutional handling - Gold Command - would include a major fire or explosion, a significant power cut, or an outbreak of a contagious disease (such as meningitis).

2. The key point is that the University Secretary should be informed immediately of any critical incident.

   During office hours he should be contacted on 0113 343 4011; at other times, he should be contacted through the Security Service (☎ 0113 343 5494 or, in emergencies, 0113 343 2222).

   If the Secretary is unavailable, his office (or the Security Service if out of hours) will contact the Deputy Secretary or another member of the core CIMT Gold Command.

3. In the event of the CIMP being activated, a meeting of the CIMT Gold Command will be convened at the earliest opportunity. Gold Command has responsibility for determining, co-ordinating and managing the University’s response to the critical incident and, where necessary, for ensuring that appropriate remedial action is taken to recover from the incident. Gold Command is chaired by the University Secretary, and consists of a core of senior managers supplemented by other staff as the occasion demands. (Further details are set out in Part 2 and Annex 1.)

Silver and Bronze Commands

Silver

4. A number of major incidents affect only one building or its immediate vicinity and can often be handled and resolved locally within a faculty or service. Such incidents are usually safety matters, often featuring a utilities problem and sometimes necessitating the evacuation of a building or buildings. Examples include a gas leak, a flood, a power outage or a local fire. The Faculty or Service would be expected to handle the matter
through the establishment of a local Incident Management Team (IMT) – a Silver Command.

5. Guidance on the establishment and operation of Silver Command is set out in Part 3. Silver Command will be coordinated on a regional basis by a nominee of the Executive Dean or Head of Corporate Service, such as a Facilities Manager (FM), where such exists, or by a local senior leader.

6. Security will ensure that Gold Command is notified of any incident being handled by a Silver IMT (so that an assessment can be made of what, if any, institutional support is required).

Bronze

7. Many incidents are contained to a small area of a single service (such as in an office or a laboratory), and can be resolved using routine local processes, perhaps supported by security or the local health and safety representative(s). Examples of minor or small incidents might include the use of a spill kit to clean a chemical spill, or responding to a fire alarm activation.

8. Although these matters can be thought of as Bronze incidents, they will be overseen by the FM or academic or service lead (as nominated by an executive dean or head of corporate service), who can advise on the support required and will escalate through Silver Command where necessary.

Communications and management information

9. As part of an immediate response (at any level of Command), the University (through the CIMT) needs to be able to contact individual members of staff, or groups of staff, outside normal working hours. The main tool for securing that end is a telephone cascade system, a key feature of the CIMP. Under that system, the Secretariat and Security Services hold out-of-hours contact details for the senior leadership of the faculties, schools and services, and for a number of other key staff responsible for buildings and other key resources (see Annex 2). Those contacts (and deputies when they themselves are not available) need in turn to be able at all times to contact all members of staff in their areas of responsibility.

10. The University also needs to be able to secure access to management information (including, for example, data on individual students) at any time and in any circumstances (even if, for example, an emergency of some sort prevents access to administrative offices). IT, SES and HR have key roles to play in maintaining institutional information in this regard, but deans and heads of schools and services also need to consider whether they hold any records peculiar to their areas of responsibility which need to be stored in duplicate (with the back-up copy kept in a different location from the first). The role of central managers is described in more detail in Part 2, and further details of the responsibilities of local managers (faculty deans, heads of schools and services) are given in Part 4.

Maintenance of the CIMP

11. Overall responsibility for the CIMP rests with the University Secretary. He is responsible in particular for ensuring that the CIMP is reviewed regularly, and that other officers are aware of their own responsibilities under the plan. Questions of policy or interpretation should be referred to him or, in his absence, the Deputy Secretary.

1 David Wardle (☎ 0113 34 34452; d.wardle@adm.leeds.ac.uk).
Part 2: Corporate management – Gold Command

This section outlines critical incident management structures and communication lines at the corporate level. In particular, it gives the composition of the (Gold Command) Critical Incident Management Team; sets out arrangements for the establishment of a major incident control centre; and enunciates guidance on communication lines.

The Critical Incident Management Team

12. The core members of the University’s CIMT Gold Command (which is chaired by the University Secretary) are:
   - Roger Gair, University Secretary
   - Francesca Fowler, Human Resources Director
   - Dennis Hopper, Director of Facilities Management
   - Jane Madeley, Chief Financial Officer
   - Mark Devane, Communications Director
   - David Wardle, Deputy Secretary, acts as secretary to the Critical Incident Management Team (CIMT)\(^2\)

(Sir Alan Langlands, the Vice-Chancellor, may choose to join at any stage.)

13. The core membership of the CIMT will be augmented as necessary, depending on the nature of any particular critical incident. In any event, the CIMT will be supported as appropriate by:
   - Paul Veevers, Director of Health and Safety Services
   - Stewart Ross, Director of Commercial and Campus Support Services
   - Steve Gilley, Director of Estates
   - Jim Slack, Director of IT
   - Linda Mortimer Pine, Deputy Director of Human Resources
   - Executive Dean or Head of Corporate Service
   - Ian Robertson, Director of Residential Services
   - Joanne Hynes, Asst. Director of Commercial and Campus Support Services
   - Malcolm Dawson, Security Services Manager
   - Catherine Lorigan, Director of Student Operations
   - (Currently vacant): Director Student Opportunity
   - Chris Warrington, Head of Student Support

14. Clerical support for the CIMT will be provided by the Secretariat, assisted by other offices as necessary.

15. Members of the CIMT (and others listed in Annex 1) are required to provide the Secretariat with their contact details, as well as those of a deputy in the event of their absence.

\(^2\) He also has responsibility for ensuring that appropriate facilities are made available to the CIMT.
16. Appropriate training will be provided to the key staff required.

Contacting the CIMT

17. Contact details for members of the CIMT appear at Annex 1, but, in brief,

(a) out of normal office hours, details of any critical incident should be conveyed to Security Services on 0113 343 2222 (emergencies) or 0113 343 5494;

(b) during office hours details of any such incident should normally be conveyed to the University Secretary on 0113 343 4011 or, failing that, to any other member of the CIMT or to Security Services (see above).

Initial meeting of the CIMT

18. Following activation of the CIMP, the first meeting of the CIMT will include the following agenda items as necessary:

(i) Situation report and formal activation of the CIMP.

(ii) Augmented CIMT as needed.

(iii) Liaison with external bodies as appropriate (e.g. police, other emergency services, the hospitals, public health and the civic authorities – a list of useful numbers is set out in Annex 1).

(iv) Initial assessment of the likely impact of the incident upon the functioning of the University (and commencement of incident log).

(v) Communication strategy, both internal and external.

(vi) Assessment of resource implications, including any need for:

(a) alternative accommodation – residential and business;

(b) additional staffing – impact on usual University activities

(c) emergency procurement arrangements and;

(d) equipment above and beyond that referred to in this plan.

(vii) Legal and insurance implications.

Critical incident control centre

19. In the event of a critical incident, some or all of the following rooms in the Marjorie and Arnold Ziff Building will normally be used as the University’s critical incident control centre: Room 13.13, the Council Chamber and Room 12.07. Both the Chamber and Room 12.07 have multiple data/phone points.

20. As an alternative, the main meeting room in the Liberty Building – which has a separate power supply from the rest of the University campus – will be utilised as the control centre.

21. When access to campus venues is not possible, Devonshire Hall will be used as the critical incident control centre.

22. In the event of a protracted critical incident, responsibility for providing food and refreshment for those managing the incident will lie with Catering and Conferencing.
Lines of communication

External communication: the media

23. In the event of a critical incident, responsibility for dealing with media enquiries will lie with the Communications Director in consultation with the CIMT (and the University Secretary in particular). The Communications Director will arrange key interviews with the Vice-Chancellor or other members of the CIMT or give interviews individually as appropriate. As a general rule, only staff trained in media relations should give radio and television interviews.

Internal communication

24. In the event of a critical incident, the CIMT will be responsible for ensuring communication as necessary with University staff. It will use some or all of the following means as a way of communicating with staff depending on the nature of the incident and the number of staff to be contacted:

- direct contact by phone or email
- placing information on the University’s web site
- local radio and press
- use of the University’s emergency telephone cascade system (see below).

Telephone cascade system

25. As is explained above, the telephone cascade system is a key component of the CIMP. If the cascade system needs to be used, members of the CIMT will as necessary - depending on the nature of the incident - contact heads of schools and services (as listed in Annex 2) to advise them to activate their local cascade systems.

26. In the event of a major incident, remote access to the University’s network servers and use of the telephone network may need to be managed. When activating the telephone cascade system, the CIMT will advise heads of schools and services on any access restrictions.

Management information

27. IT is responsible for ensuring ready access to management information held centrally on its systems on the basis set out in their critical incident and disaster recovery plans.

Testing of the plan

28. Arrangements will be made to test the Gold Command plans on at least an annual basis.

---

3 It should be noted that a more comprehensive emergency communications solution is currently being considered by the University. The arrangements in paragraphs 24-26 apply in the meantime.

4 In normal circumstances only a limited number of users can access Desktop Anywhere at any one time. (Remote access to email accounts via Office 365 is unlikely to be limited.)

5 In the event of a major power outage, the University telephone network will run, for a limited period of time, on its battery power back-up supply.
Part 3: Silver (and Bronze) Command

This section outlines the steps that should be taken to establish a Silver Command Incident Management Team to deal with serious incidents at a local level.

The Incident Management Team (Silver Command)

29. Where Security determines that an incident can be handled locally, they will notify the responsible Facilities Manager (or senior leader), who will convene the local Incident Management Team Silver Command. (Security will also be responsible for notifying Gold command of any emerging crisis or pattern of crises.)

30. The core members of the IMT Silver Command are:
   - Executive Dean of Faculty or nominee
   - The Facilities Manager
   - (Relevant) Heads of Schools or Services
   - Faculty Health and Safety Manager
   - Faculty Human Resources Manager
   - Faculty Finance Manager
   - Faculty Education Services Manager
   - Malcolm Dawson, Security Services Manager

31. Silver Command IMT will be established in the event of an incident as described in paragraphs 4-6 above. That is, for major incidents that affect only one building or its immediate vicinity and can often be handled and resolved locally within a faculty or service. The IMT’s membership will be augmented as necessary, depending on the nature of any particular critical incident; and, in any event, advice can also be sought from Security, who will consult member(s) of Gold Command where necessary.

32. Arrangements should be made locally to establish an incident meeting room and for administrative support to the IMT.

33. The Facilities Manager or other nominee will coordinate the relevant sub-sector of the IMT to respond to those minor (Bronze) incidents that are contained to a small area of a single service (such as in an office or a laboratory), and can be resolved using routine local processes (see paragraph 7 above).
Part 4: Local responsibilities

34. The overall responsibilities enumerated in Part 3 are likely to rest with the relevant executive dean or head of corporate service (assisted by the relevant Facilities Manager). The executive deans or heads of service must therefore take especial care to satisfy themselves that any arrangements made at school or departmental level are consistent with these notes, and are generally appropriate and adequate.

35. A few specific corporate services - IT, Estates and Residential Services - which have campus-wide responsibilities are expected to maintain their own local CIMP's. Other areas may wish to consider their own management arrangements but, as a minimum, the University requires each unit\footnote{Where ‘unit’ refers to school or service. Separate supporting guidance will also be issued on the arrangements required locally.} to:

(a) devise an effective local response to a critical incident which includes a \textit{telephone cascade system}; and

(b) return specified information to the University centrally, including \textit{safety critical information}.

36. Staff should also be invited at least once a year to have an input into critical incident planning and, in particular, given the opportunity to identify any types of critical incident to which the faculty, school or service area may be particularly susceptible and for which it might not have appropriate contingency plans. Such discussion might best be set in the context of the overall risk management arrangements for the area.

Local response

\textit{Telephone cascade system}

37. Head of units are required to maintain an up-to-date telephone cascade system so that, in an emergency, all members of their staff may be contacted out of working hours. (The system would only be used to communicate with members of staff in a real emergency – or when their normal places of work are shut or remote access to the University’s network needs to be restricted.)

38. The telephone cascade should include both home and mobile numbers and, whilst its precise design is for the head of units to determine, it should be constructed in such a way that a call can be made to all members of their staff within 30 minutes of the cascade being activated.

39. The cascade system also needs to be constructed in such a way that it does not depend on particular individuals being available when a critical incident occurs. This means that each school or service should nominate at least four individuals who are designated \textit{‘telephone cascade key contacts’}. These contacts:

(a) will be senior members of staff, with the authority to activate the telephone cascade at the request of the CIMT, and to adjust its workings to take account of the pattern of staff availability at the time; and

(b) will need to lodge their own telephone numbers with the Secretariat.

40. \textit{It is essential that all staff are made aware of how the telephone cascade system will be implemented in the event of a critical incident, and that they have the necessary information to fulfil their own particular role in the cascade process.} The telephone cascade needs, of course, to be kept up-to-date; and head units should ensure that it is
systematically reviewed at least once a year. Occasional ‘trial runs’ of the system will be arranged.

**Returning information to the University**

41. Head of units are required to provide the Secretariat with:

   (a) an up-to-date list of at least four **telephone cascade key contacts** who can activate the system; and

   (b) an up-to-date list of at least four **site contacts** (who can be reached out of hours) to provide site-specific information.

42. ‘**Site contacts**’ are designated staff who are able to advise Security Services of any safety critical information about their area of responsibility (such as the storage of dangerous substances, access to rooms and the making safe of particular equipment/machinery).

43. The Secretariat will be responsible for ensuring that the records are up-dated as necessary (for use by Security Services as and when required).

**Protecting information and assets**

44. Consideration must also be given as to how best to protect assets should a critical incident (such as flood or fire) occur. (Further guidance will be issued in due course.)
Contact information

Out of normal office hours, details of any critical incident should be conveyed to Security Services on 0113 343 2222 (emergencies) or 0113 343 5494 (normal number). Security will then contact members of the CIMT and other staff as necessary.

During office hours, details of any such incident should normally be conveyed to the University Secretary on 0113 343 4011 or, failing that, to Security Services (who will contact the Deputy Secretary or the Director of Health and Safety Services as necessary).

Internal extension numbers for members of the CIMT are given below for ease of reference. (Security Services holds numbers for contacting all of these individuals out of hours.)

Critical Incident Management Core Team
Roger Gair, University Secretary 34011
Francesca Fowler, Human Resources Director 36644
Dennis Hopper, Director of Facilities Management 36080
Jane Madeley, Chief Financial Officer 36000
Mark Devane, Communications Director 33207
David Wardle, Deputy Secretary. 34452

Other key individuals
Sir Alan Langlands, Vice-Chancellor 33000
Paul Veevers, Director of Health and Safety Services 34207
Stewart Ross, Director Commercial and Campus Support (CCSS) 36078
Joanna Hynes, Assistant Director CCSS 35490
Steve Gilley, Director of Estates 38363
Malcolm Dawson, Security Services Manager 35490
Catherine Lorigan, Director of Student Operations 33998
Ian Robertson, Director of Residential Services 36366
Jim Slack, Director of IT 37087
Aidan Grills, Chief Executive of Leeds University Union 0113 380 1408
Beverley Kenny, Head of Catering and Conferencing 33680
Chris Warrington, Head of Student Support 34075

External bodies
Police, Fire and Ambulance services 999
Hospitals Leeds General Infirmary 0113 392 2512
St James’ 0113 206 4478
NHS Inquiries 111
City Council all services 0113 234 8080
out of hours 0113 247 8500
emergency planning unit 0113 247 4513
Principal services (usually contacted via Estates Services)
Yorkshire Electricity 0800 375 676
Transco (Gas) 0800 111 999
Yorkshire Water 0845 124 2424
Public Health – Health Protection Unit

Health and Safety Executive

Environment Agency
- information on floods and flood warnings
- reporting pollution and environmental damage

Leeds Beckett University – Secretary’s Office

BBC emergency service
(Data held centrally)