Crisis communications: guidance document

Crisis communications is a key element in effective crisis management. Its role is to help ensure the continued operational effectiveness of an organisation during and after a major incident, provide guidance and reassurance to those affected, and safeguard the organisation's reputation.
This document provides guidance on:

1. major incidents (eg fire, explosion, security threat): what action you need to take to ensure you are prepared for a major incident and advice on communications activity during an incident;
2. reputation management: advice on communications activity when something has occurred which threatens the reputation of a unit or organisation.

It considers three key stages in dealing with crisis communications:
1. preparation in advance of an event
2. communications activity during a major incident
3. follow-up after the initial incident has passed.

In the event of a University-wide crisis, particularly where the University's Crisis Management Plan is activated, the Public Affairs Directorate will lead the communications response across the University's main channels (including web and social media) with all key audiences, such as the University community, the news media, the general public, and important community and political stakeholders.

However, even where a crisis or emergency event is localised, it is critical that you contact the University's News & Information Office in the Public Affairs Directorate as soon as possible (see back page for contact details). The team will deal with all news media activity on behalf of individual departments and colleges.

1. Major incidents

Communications and contingency planning
Planning is fundamental to the success of effective crisis management. Crisis communications should form part of the business continuity and contingency planning process for each area.

As part of your contingency planning, think through the practicalities of communicating in an emergency. How would you communicate internally and externally if the crisis took IT and phone systems down or made your offices unusable?

- Which communication channels would you be able/unable to use, and what's your back-up?
- Is there an alternative office you can use? What equipment do you need in it?
- Can staff access communications channels from home? Can they remotely access University email, voicemail, files and shared networks? Consider who should have remote access via the Connect Remote Desktop Service or similar systems.
- Can those people tasked with issuing communications:
  - send mass emails from home/a remote location?
  - remotely publish to the website and/or the intranet?
- Can you operate outside the University IT and phone systems?
  - Do you have mobile numbers for all the key people? Are chargers available in the office?
  - Do you have personal email addresses for all the key people?
- Are conference call facilities available so that all the key people can talk together during a crisis?

Prepare contact sheets

If you only do one thing to prepare for a crisis, make it this!

- List the key people who would need to be:
  (i) involved in the management of an incident;
  (ii) informed immediately about an incident.
  Include in your list key managerial and operational staff (eg IT support, Health and Safety), as well as central University contacts (eg News & Information Office, Security Services – see back page for contact details).
- Ensure you have up-to-date mobile and home phone numbers for all key people.
- Ensure you have personal email addresses for all key people in case your email system goes down.
- Work out the cascade through which breaking information will be communicated to the list. The top of the cascade is 'person X', ie whoever on the list hears about the incident first.
- Distribute the cascade structure and full contact details to everyone in the cascade.
- Ensure you hold an up-to-date mailing list for all students and staff of your department/college.

Identify your potential audiences

- Who would be directly affected by an incident (eg staff/students in the building) and who would be indirectly affected (eg people in neighbouring buildings, parents of students)?
- What information would they need?
- Where would they get those messages (eg online, email, the news media, social media)?
- What about external audiences who would be interested but not affected (eg prospective students and staff, donors, alumni, funding bodies)? How would you communicate with them?
- A serious incident will certainly attract media attention. Make sure you inform the News & Information Office straight away in the event of an incident and use them to help manage the news media.

Plan your channels

- What are the communications channels you'll need to use in a fast-moving situation (eg email lists, TV display screens, social media, websites)?
- Do all relevant staff know how to access these, remotely if necessary, including logins and passwords?
- Some of your audience may not have computer access (either generally, or if systems are down in an emergency). How will you communicate with them?
- If the incident is isolated to your department/college, do you need to think about the volume of calls from people ringing through for the latest information?
- Ensure all contact details, crisis plans and materials are available in multiple places: in mobile phones, on computers, on memory sticks, uploaded securely to the web and on paper. You never know when and where you'll need them.

Prepare draft material in advance

- If there are known risks with predictable consequences, prepare draft material in advance.
- Ensure that your department/college's up-to-date emergency plan and business continuity plan includes communications and that your communications planning is consistent with these.
- Prepare an incident update template for use on email and/or other channels. Include update number, date and time so the sequence and recency is clear.

Identify sign-off and roles well in advance

- Time will be critical and organisational leaders will be tied up. Ensure communications professionals are empowered to act during an incident.
- It is essential that a light-touch sign-off process for crisis communications content is agreed. Aim for no more than one person to be checking and signing off content.
- Ensure that, in the event of disagreement, a single person has ultimate decision-making power.
- Identify who will be in charge of communicating, and plan for that person to have both the authority and the information to communicate as events unfold (not after the fact).
- Identify who will be the key spokesperson in a crisis. Will this person appear on TV/radio if necessary? Do they need to be media trained? Who will deputise for them if they are not available?
- Ensure a clear chain of command so that if anyone is out of action their authority is passed to someone else.
- If the University's Crisis Management Plan is activated, you must follow the sign-off and decision-making structures outlined in the plan or set down for the specific incident.

Planning for reputational risk

An incident may impact on the University's reputation in two ways:

- sometimes a crisis is purely reputational: information has gone into the public domain that casts a negative light on the unit or organisation. This might be a negative issue already known to you that had not been public until now or that only becomes known to you at the point of becoming public, even though it happened some time ago;
- an event that threatens/involves a physical threat (eg explosion, flooding, fire) may have a reputational impact if it is badly handled or gives rise to inaccurate information about the University's role or involvement.

It may be possible to identify risks in the first category in advance. This is not simply a matter of identifying those things you believe your unit/organisation is doing wrong – it could be anything that the public might perceive as negative. This can include things that, although above board, are unpopular with the public, or things that are uncontroversial when understood properly but which are liable to misunderstanding.

- Once you have identified the reputational risks, try to assess priority: decide which risk(s) to mitigate most urgently. Red flags are:
  - anything where there has been genuine wrongdoing;
  - anything likely to command national-level media interest.
- Mitigate reputational risk in advance.
  - If the reputational risk relates to something that is genuinely wrong, the first course of action should be to correct it. If correcting the problem is a long process, you will also need to put shorter-term mitigation in place.
  - Prepare draft statements and Q&As (with the News & Information Office) that you would use if the issue became public. These should follow the process outlined below for preparing media responses.
  - Sometimes preparing these responses reveals that there would be useful facts and figures to back up your points that are not currently collated (eg figures on the national picture that put your figures in context). Do the work now to get them together.
  - If you have identified things that are uncontroversial when understood properly but which are liable to misunderstanding, can you act now to explain them more clearly to the public, for example on your website?
- Decide in advance in consultation with the News & Information Office who will be the key spokesperson for broadcast interviews should an issue break in the media. Do they need to be media trained?

Make sure people know about the plans

- Communicate all the plans, contacts and materials to your crisis team members.
- Brief new staff and remind staff regularly.
- Hold an annual crisis exercise to test your plan, then revise your plan accordingly.

2. Activity during a major incident

Crisis communications checklist

- ✓ Inform the University News & Information Office in the Public Affairs Directorate as soon as possible and use them as the conduit with the media.
- ✓ Ensure the mobile phones of all key operational people are switched on and charged.
- ✓ Implement your communications cascade/call-out procedure.
- ✓ Establish key facts and agree key messages.
- ✓ Log all decisions made and keep a record of all communications activity.
- ✓ Issue regular updates to key audiences – include update number, date and time so recency is clear.
- ✓ Set up regular team debriefs for all key operational people.

Key elements to your communications response

Getting communications right in the first few hours, especially with the media, is critical. Rumour will fill a vacuum so don't think you can put out the fire and then communicate that you have put it out. You need to communicate alongside managing the incident.

Inform the News & Information Office as soon as possible and use them as the conduit with the media. Where communications are being managed by the Public Affairs Directorate, simply link to, re-post or re-tweet the messages they distribute via web, social media etc. Otherwise, follow these basic principles:

- Maintain a 'single source of the truth' – a document containing key facts and messages. Use this as the basis for all your communications.
- Review this as new information comes to hand to ensure your facts and messages remain accurate, relevant and appropriate.
- Keep a log of all risks, actions and decisions and ensure it is regularly updated as the crisis event unfolds.
- All crisis communications should follow these principles.
  - Empathetic: showing the University understands how a crisis impacts staff, students, their families or members of the local community, and accepting blame and apologising unreservedly where it is demonstrably at fault.
  - Transparent and responsive: any response should be accurate, timely, consistent and courteous, even when faced with hostility.
  - Action-focused: providing reassurance by outlining what the University is doing to take control of the situation, either itself or in conjunction with other agencies, and giving examples where possible of actions already taken. Key phrase: 'I want to reassure you that we are taking control of this situation and as soon as we have any news we will update you.'
- Where information is not yet available, tell your audiences this rather than saying nothing or saying things that are unconfirmed and that later need to be retracted or corrected.
- Work closely with the Public Affairs Directorate to ensure your key spokesperson is fully briefed and has the latest information.
- Correct misinformation and scotch rumours promptly.

Manage your communications team

- Keep each other informed. If possible, get all the key people to catch up for ten minutes in each hour, ideally face-to-face but otherwise on a conference call.
- If a crisis is likely to extend beyond a single working day, put a rota in place to ensure that there are always qualified people available or on-call and that everyone gets a break.
- Once the worst of the crisis has passed, ensure those involved are thanked; acknowledge difficulties and stress for all those affected.

Reputation management

Many of the same communications principles used in major incidents apply here. The most important are:

- let the News & Information Office know immediately of a significant reputational risk (whether or not it has become public);
- involve the News & Information Office in any communications with the news media;
- identify potential reputational risks and mitigate them where possible;
- plan in advance for these known reputational risks by preparing reactive material; and
- ensure that you can communicate at speed and that you have an agreed sign-off process.

When an issue breaks in the media

Usually you will be contacted by a journalist in advance of a story being published or aired and given an opportunity to comment. Involve the News & Information Office immediately. Depending on the severity of the reputational risk, the News & Information Office will either lead on handling it or will take an advisory role (NB anything being covered by a national or international media outlet should be seen as a serious reputational risk).

Before publication/airing: preparing a response

Important principles:

- Know the full truth (and the News & Information Office must be given the full truth): any reputation management strategy must be informed by the full, unvarnished facts, including any that do not directly pertain to the specific question but could become relevant if the story broadens.
- Act fast, but ensure factual accuracy.

Responses would usually be given in writing (as a statement). The News & Information Office will take you through the following process.

- Establish the media agenda: Different media outlets come with different political stances. What is the agenda? What story do they want to tell? What else is topical that this may play into? Who else will enter the public debate and what will they say?
- What is the damaging headline? The question is not which facts are objectively the worst, but which feed into the most attention-grabbing and negative headline. You need to deal with the hypothetical headline, not the facts as you know them. If you were a journalist for this media outlet, what headline would you be aiming for?
- What's the evidence for that headline? What facts, or indeed falsehoods/potential misunderstandings, exist that would support that worst-case headline? How likely are they to be acquired and used by a journalist?
- Is this evidence sound?
  - If not, show it: often the apparent supporting evidence for a worst-case headline is actually a misunderstanding, or even a falsehood. You need to spell this out very clearly and robustly. Perhaps the figures that seem to tell a bad story are simply wrong, or taken completely out of context.
  - If yes, give any balance or mitigation: maybe the evidence for the damaging headline is sound, but the journalist does not have the context for it. This context or mitigation must be given to the journalist and passed on to their audience.
  - If there is no balance, apologise: if the story is a 'fair cop', the best way to manage reputation is a frank apology and an explanation of what measures will be put in place to stop something similar happening again.

Time is of the essence

- In managing a crisis, time is crucial – this is particularly true for a reputation crisis. Once something has gone into the mainstream media and social media, it can quickly be seen as 'established truth' and will be extremely difficult to undo. The longer it stays there uncorrected, the more it hardens into the accepted history of the situation and of your institution.
- You must act quickly to correct this misinformation and protect your and the University's reputation, first by doing everything you can before publication or airing – in what may be a matter of hours or even less in which to respond – and by acting rapidly afterwards.

3. Follow-up after the initial incident

Follow-up after the initial incident

Depending on the scale, there may be little follow-up required beyond the initial incident. However, you should assume that there will be some ongoing activity that will need to be managed in addition to business-as-usual work. Consider:

- Is there likely to be ongoing interest? Consider key dates or events (eg reopening of a building, publication of any review into the incident).
- If the incident has caused ongoing disruption to your departmental/college/service activities, how will you keep people informed of interim arrangements and progress with managing the aftermath?
- How will you reassure key stakeholders once you are back to 'business as usual'?
- What have you learnt from the event? Do you need to amend or revise your crisis communications plans in light of practical experience?

Central University contacts

University News & Information Office: 01865 (2)80528/07738 135619
Security Services: 01865 (2)89999
Occupational Health: 01865 (2)82676
Safety Office: 01865 (2)70811
Insurance team: 01865 (6)16078
(in the event of damage to University property)