3.5. Online UCC

In 2016–17, 87% of Australians were internet users. Social networking, shopping and banking were equally popular online activities – with each attracting 80% of internet users.

It is not surprising that people are increasingly using social media platforms to express their views and opinions about issues. A survey in the United Kingdom found that one in four social media users used platforms such as Facebook, Twitter, Instagram or Google+ to make a complaint over a three-month period.

People have a right to complain about an issue in the way they want to, including online. Online complaints are only problematic when justifiable complaining becomes inappropriate and/or involves unlawful attacks on organisations and their staff. This type of behaviour can cause serious psychological or reputational harm because it can be very public and often vicious, and must be dealt with decisively and swiftly – in the same way as other more traditional forms of UCC.

3.5.1. When does online conduct become problematic?

If online conduct occurs during or as a direct result of services provided or work done by an organisation or its staff and is considered to be unacceptable (and in some cases unlawful), then it can legitimately be characterised as UCC and must be dealt with as an organisational issue. However, the level and type of response needed will vary depending on the circumstances of each case.

Some examples of inappropriate and unreasonable conduct by people complaining online include:

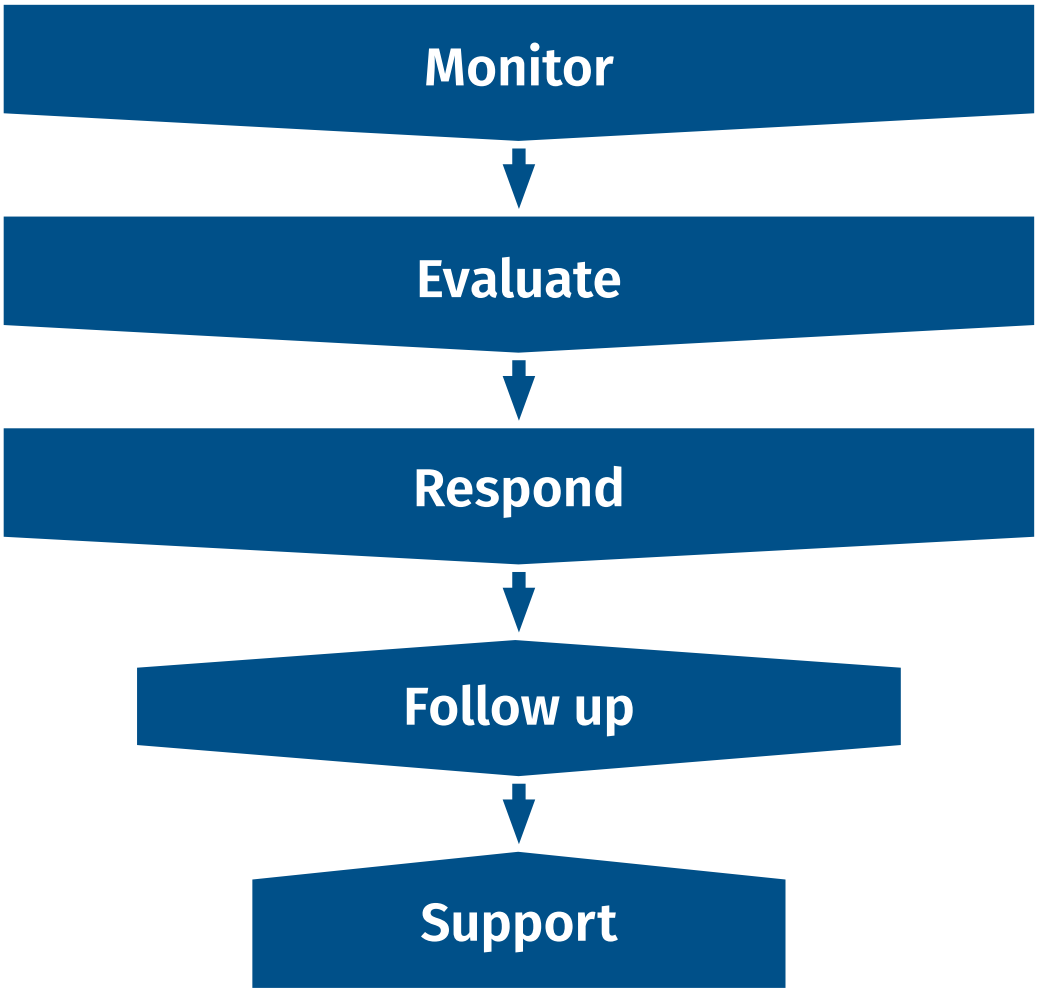
- Posting lies and defaming organisations and their staff (and in some cases their family members) – such as making corruption allegations or commenting about their personal lives or alleged sexual activities.
- Creating unpleasant websites with rude comments, photos or videos depicting members of an organisation or their family members.
- Stalking (repeated attempts to make contact/unsolicited or unwanted communications) or bullying (creating pages or online groups targeted at an organisation or its staff).
- Sending messages or posting comments that contain harassing or offensive language – including sexual references, inappropriate nicknames or jokes, racial slurs, rude or deliberately offensive comments.
- Ridiculing organisations and/or their staff to intentionally embarrass or humiliate them or worse.
- Conducting snide online polls about organisations and their staff.
- Sending threatening, harassing, verbally abusive or confronting messages/comments/emails/posts.
- Posting personal information about staff members of an organisation – including their phone number or contact details, name, address or vehicle details.
- Posting links to other disreputable or inappropriate websites, and hacking or uploading viruses or other materials that are harmful to an organisation's network.
- Posting comments to incite others – including encouraging illegal activity or engaging in violent conduct towards a staff member.

- Using an automated system to repeatedly send the same message to your network so that it overloads or crashes.
- Altering or misrepresenting information or correspondence from an organisation or its staff, inappropriately using an organisation's trademark or letterhead or otherwise violating copyright laws. This usually happens when online comments and postings are copied by a complainant to appear as though they are their own.
- Creating fake online profiles to impersonate someone or so that they cannot be identified (anonymity).

3.5.2. Taking a risk management approach to online UCC

Employers need to adequately protect themselves and their staff from risks to health and safety and liabilities that can happen as a result of online and electronic communication. Preferably, this should happen whether or not an organisation has a social media or online presence and should include clear protocols and procedures for dealing with UCC in e-communications. These protocols may be part of a broader UCC policy or can be a separate document. They should include a risk assessment process to help staff to determine when and if so how to respond to UCC in such situations.

The following risk assessment process is largely based on the work of Mike Kerwin, executive writer at Levick Strategic Communications LLC and Alyssa Gregory, founder of Avertua LLC.



Step 1 – Monitor

Maintain

- an ongoing system for researching and keeping track of postings and online comments about your organisation and staff.
- Encourage all staff to report any inappropriate or questionable online content that they discover which relates to your organisation or a member of your staff.
- Use online listening tools and alerts – such as Google Alerts, Social Mention, Technocrati, TweetBeep and Boardtracker etc. Google Alerts, for example, can send email updates of the latest online mentions about your organisation whether it is on a blog, a news item, in a video or tweet – eliminating the need for manual searches.
- Designate an authorised staff member (or response team) to monitor online content. This person should also be responsible for evaluating identified online content and deciding whether a response is needed – and if so what that response will be.

Step 2 – Evaluate

Once you are aware of the online content, the next step is to look at what response, if any, is needed. It is essential that this occurs promptly so that you can avoid or minimise the likelihood of these situations spiralling out of control. The following issues may be considered:

Content

- Does the online content contain constructive criticism, an observation or negative criticism?
- Is the online content relatively moderate in its tone or does it contain grossly inflammatory or offensive content that will require some form of action?
- Is the online content grossly misinformed or misleading or does it contain misrepresentations or lies that could reasonably mislead others?
- Does the online content contain personal information about staff members – such as their names, photos, videos, contact details (personal or at the organisation) or any information that could be used to identify the staff members or members of their family?
- Does the online content contain defamatory information or threats, violate trademark or copyright laws, or contain otherwise unlawful content?
- Does the online content contain profane, indecent, vulgar or obscene sexual content and/or unsubstantiated allegations about staff?

Apparent purpose/objective

- Does the online content appear to be dedicated to degrading others? Is it part of a smear campaign or a publicity stunt?
- Does the online content incite others to engage in a particular act or omission – such as boycotting your organisation or taking part in illegal conduct?
- Does the online content appear to have been created with the intention to embarrass or humiliate or as part of a joke?
- Does the online content seem to have a valid basis – raises a valid issue for which you or your staff are responsible and should take steps to rectify?

Visibility and credibility

- Is the online content on a website that is highly visible and easily accessible? For example, is it on Facebook (with approximately 16 million Australian users) or is it on an obscure website that has been viewed by a relatively small number of people – the person's inner and/or extended circle of friends and family?
- Has the online content taken on a life of its own – possibly even being reported in the news media and therefore requiring a relatively comprehensive response?
- Could the online content be perceived to be credible or is it so farfetched that it will not be believed by a reasonable person?

Impact

- Could the online content significantly damage your organisation's reputation or that of a staff member?
- Is the online content having (or likely to have) an impact on your workplace environment, on relationships between colleagues or with people who have made or may make complaints, or on cohesion in the workplace? If so, some form of action will be required.
- If the online content is about a staff member, how do they feel about the posting? Have they (or their family) been affected by it in a substantial way?
- Could your organisation be open to duty of care, WHS or legal issues if some form of action is not taken in response to the online content?
- Could the online content be interpreted as a representation made by or on behalf of your organisation? Has the person represented themselves as a member of staff or another relevant authority figure?
- If relevant, is the person hijacking the communication stream in a way that is affecting its effectiveness or the ability of other people to use it in the intended way? This applies if your organisation is running a blog, Facebook or Twitter page or other online communication stream.

Context

- What is the timing of the online content? For example, has it been created at a time when your organisation (or a staff member) is under unusual public scrutiny – for example, because of a highly controversial report or for inappropriate conduct? If so, a response may be needed for 'damage control'.

Step 3 – Respond

Is a response needed?

If a response is required, it should be done promptly – within hours if not minutes of the online content being identified – before it has a chance to be picked up and spread widely. A timely response can also be pivotal to whether or not you can defuse the situation or a whether a comment spreads out of control.

Depending on the circumstances, reasons for responding to online content could include that:

- there is a significant risk that the online content could mislead others – because it contains gross misrepresentations or is highly misinformed
- it is extremely inflammatory, offensive, defamatory or otherwise unlawful

- it could cause significant reputational and psychological harm
- it discloses highly personal information about staff or their families or would give rise to legal or WHS issues for the organisation if it is not acted on
- it is highly visible and accessible, has gone or could go 'viral'
- it appears to be credible even though it is not or could cause others to be grossly misinformed
- it is having a significant impact on the workplace and relationships between colleagues and with people who have made or may make complaints
- it has been created at an inopportune time for your organisation.

There are a number of options for responding to online content. Responses can be public or private, they can take the form of a comment, a rebuttal or rejection, or they can include a statement on the website or forum where the inappropriate online content was discovered, or on your organisation's website, or be delivered by email, a telephone call, a face-to-face interview or in a letter. The most appropriate method for response will depend on the circumstances of each case.

Should it be a public or private response?

When deciding whether a response should be public or private you may consider the following issues.

Public response

If the online content is on a website that is highly visible and accessible or includes gross and repeated false and misleading information, a public response may be appropriate. A public response can either be done on the website where the offending online content was discovered, on your organisation's website, blog or social media page, or in an online newsletter etc.

It is important for public responses to be unemotional. They should show restraint and treat the complainant with dignity and respect.

Public responses should offer to correct problems if your organisation or staff have done something wrong. If all else fails, responses should thank the person for their comment and move on as quickly as possible. The reality is that the public audience is more likely to be looking for how you respond, rather than the person who posted the online content. If you respond badly, then you will do more damage than the person who posted the content ever could do.

The following suggestions have been taken from Robert Bacal's *Defusing Hostile Customers Workbook*. Bacal suggests that these are the most effective layouts for responding to people through electronic mediums, including posts on social media websites, to ensure that your key messages stand out and that readers see them quickly and pay attention to them. These suggestions can also minimise the likelihood for misunderstandings:

- Use short paragraphs, with double spacing between each paragraph. Six to ten lines per paragraph.
- Use short sentences and simple sentence structures. Complex structures will be even more confusing online than on the printed page.
- Use proper headings – assume your reader is going to take a quick look at the page overall to see if what they are looking for can be found in the headings.

- Make sure that the main content of the page is readable without scrolling down the page. That does not mean that everything that is important needs to be at the top, but it does mean visitors should be able to quickly see what is on the rest of the page by looking at the top.

Once you have responded publicly, shift to private responses/correspondence with the complainant by email, telephone or face-to-face.

Private response

If the online content is not publicly accessible, then a private email response, letter or phone call may be appropriate and adequate. A private response can be used to clarify issues – including when your organisation or staff have done something wrong – or to give the person who posted the content an opportunity to remove the online content before taking more decisive action. The latter should always be done in private because it could be viewed negatively online.

Both public and private responses

If the online content has taken on a life of its own and has spread virally across the internet or other communication platforms, a more comprehensive response strategy may be required. This response strategy could include press and/or media releases and interviews, proactive outreach to relevant people, corrective messaging in social media and/or on your website or blog, or responses in any other relevant publications produced by your organisation.

It can be difficult to know when an online posting or website will be picked up and spread. Online listening tools can be helpful to alert you to all mentions of your organisation. As the number of mentions about a particular issue increases, you will have an opportunity to make a comment or even deal directly with the source of the posting before things get out of hand.

No response needed

If a response is not needed, then usually no further action is required. In some cases, it may be appropriate to copy and make a record of the content to identify recurrent behaviour. It may also be important to provide assistance and support to any staff members affected by the comments.

Step 4 – Follow up and follow through

Once the online content has been responded to – either directly or indirectly – you should continue monitoring to identify new comments and track old comments to see if they are picked up elsewhere or revived.

Also, if a person's concerns were valid and/or your organisation or staff have done something wrong, consider following up with the person a couple of weeks after the incident to make sure that you have satisfactorily addressed their concerns. By keeping in touch, you convey a sense of approachability and increase the likelihood that they will contact your organisation in the first instance next time around – before turning to the internet.

Step 5 – Support affected staff members

If the online content poses a significant risk of psychological or reputational harm to staff, it may be important to consider providing the affected staff with a public message of support – as part of your public response. This message of support will be important in discrediting and rejecting the person's remarks and making staff feel (and the public recognise) that they and their work are valued and supported by the organisation. You should also take appropriate steps to make sure staff receive adequate counselling and support services.

Staff should also be advised on the legal avenues that they can take in such situations and, in appropriate cases, should be supported to do so. Depending on the circumstances, there are legal mechanisms that could be used to deal with online UCC under relevant Commonwealth and state legislation.

For example, in NSW this could include an action under the:

- *Anti-Discrimination Act 1977* (NSW)
- *Broadcasting Service Act 1992* (Cth)
- *Copyright Act 1879* (NSW)
- *Copyright Act 1968* (Cth)
- *Crimes Act 1900* (NSW), in particular Part 6 – Computer Offences
- *Criminal Code Act 1995* (Cth), particularly:
  - s 147.1 – Causing harm to a Commonwealth public official
  - s 147.2 – Threatening to cause harm to a Commonwealth public official
  - s 474.14 – Using a telecommunications network with intention to commit a serious offence
  - s 474.15 – Using a carriage service to threaten to kill another person or entity
  - s 474.16 – Using a carriage service for a hoax threat against another person or entity
  - s 474.17 – Using a carriage service to menace, harass, or cause offence to another person or entity in such a way as would be regarded as offensive by reasonable persons.
- *Defamation Act 2005* (NSW)
- *Privacy Act 1988* (Cth)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Racial Discrimination Act 1975* (Cth)

A carriage service under the Criminal Code Act is any service that facilitates communication through electronic energy. This includes telephones or mobile phone services, the internet (and any facility on it like email or social networking websites), and using facsimile or other electronic means.

Case study – An example of online UCC

A man approached an Ombudsman in 2010 complaining about an agency's investigation and review of his complaints about his former employer for breaches of work health and safety legislation. He also complained that the agency had not responded to his complaints about safety breaches in an appropriate manner and alleged that – because of the agency's negligence in not referring to the legal evidence he had provided them – he had lost his employment, finances, retirement investments and worst of all his good health.

The Ombudsman accepted his complaint and decided to make inquiries into the issues he had raised. During our inquiries, we discovered that the person had created a website about his issue.

Ombudsman staff visited the website which seemed to target the person's former employer and its board of directors, whom he compared to former Chinese Communist regimes. The website also targeted a wide range of people and organisations that had rejected his allegations and included copies of correspondence involving them along with photos – some with speech bubbles added to the photos. There were also more than 60 links on the website's home page to the correspondence he had either sent or received from these people and organisations, accusing many of them of being biased and fraudulent. A number of the letters on the website had been altered to draw attention to certain sentences which were responded to either in typed script or with scribbled comments in the margins.

The website also made allegations of taxpayer-funded sex and child abuse and made references to other controversies. This appeared to have been done to support his allegations of bias and corruption – though they were completely unrelated to his complaint. There were accusations about criminal activity and negligence, fraud, discrimination and violence among other things, and – in an apparent attempt to make the website credible – included more than 30 union, government and company trademarks and logos copied onto the website's home page. Some of these had been altered to include the name of his former employer in different fonts, colours and sizes.

The home page also had approximately 10 scrolling messages about his former employer. One bounced, five scrolled to the left, while another scrolled to the right. One scrolled upwards and another went downwards and one was identified as 'breaking news'. It even offered a $5,000 reward for any evidence on his former employer's alleged work health and safety violations and directed people to his Twitter and Facebook pages which had also been created as 'part of [his] pursuit to expose [the CEO's] OHS crimes'.