Dudley Safeguarding

protecting children, young people and adults at risk

September 2016

Cyberbullying

Advice for all individuals that work with children, young people or adults









Prepared on behalf of

Dudley Safeguarding Children Board and **Dudley Safeguarding Adults Board**

Cyberbullying: Advice for all individuals that work with children, young people or adults

Who is this advice for?

This is advice for all individuals that work with children, young people or adults, on how to protect themselves from cyberbullying by service users or those linked to service users and how to tackle it if it happens.

Overview

It is important that all organisations take measures to prevent and tackle bullying whether that is among those accessing their service or aimed at staff working within the organisation. It is equally important that organisations make it clear that bullying of staff or volunteers, whether by service users, those linked to service users (for example parents, family members, partners or carers) or colleagues, is unacceptable. Evidence indicates that one in five (21%) teachers have reported having derogatory comments posted about them on social media sites from both parents and children.

Educational establishments can offer parents and carers support on how to help their children engage safely and responsibly with social media. Further information for parents can be found at http://www.dudleysafeandsound.org/parents.html .

Creating a good relationship with service users or those linked to service users can help create an atmosphere of trust that encourages concerns to be raised in an appropriate manner. Part of this is making sure that service users or those linked to service users are aware and understand how to communicate with the organisation. Organisations should also make it clear that it is not acceptable for service users, those linked to service users or colleagues, to denigrate and bully staff or volunteers via social media, in the same way that it is unacceptable to do so face to face.

Organisations should encourage all staff, volunteers, service users and those linked to service users to use social media responsibly.

Staff and Volunteers

Staff and volunteers are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff and volunteers which may help protect their online reputation:

- ✓ Ensure you understand your organisations policies on the use of social media, Childnet's 'Using Technology' guide has more information on what to be aware of.
- ✓ Do not leave a computer or any other device logged in when you are away from your desk. Lock the device.
- ✓ Enabling a PIN or passcode is an important step to protect you from losing personal data and your own images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by service users.
- ✓ Ensure your password or PIN is known only to you. Use a 'secure' password (include mixed case letters, numbers and punctuation marks). Check your organisation's password policy.
- ✓ Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found at: http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/safety-tools-on-online-services
- ✓ It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online, it is much easier to deal with this as soon as it appears. http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation has more information on this. Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- ✓ Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- ✓ Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- ✗ Do not accept friend requests from service users past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with service users or those linked to service users and therefore could read your post if you do not have appropriate privacy settings.

- ✗ Do not give out personal contact details – if service users or those linked to service users need to contact you for any reason, always use your work contact details. When working with individuals away from the usual work place (for example day trips / residential etc), staff and volunteers should have a work mobile phone rather than having to rely on their own.
- ✓ Use your work email address for work business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

If you are bullied online

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a service user, linked to a service users or a colleague, the majority of cases can be dealt with most effectively through the organisations own procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse, it should be an organisational decision what to do next – either the organisation or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example: http://www.saferinternet.org.uk/
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the organisation may consider contacting the local police. Online harassment is a crime.

Responsibilities of organisations

Employers have a duty to support staff and volunteers; no-one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if appropriate.

The Professional Online Safety Helpline (see page 5) is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline

provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example, cyberbullying or sexting issues.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

All employers have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by service users, those linked to service users and other members of staff, supporting them if it happens.

Reporting

Everybody within the organisation should understand reporting routes and responsibilities. Many organisations will appoint a designated person to deal with bullying, while others will distribute responsibility among a number of staff.

West Midlands Police Response

If the bullying amounts to harassment (alarming the person or causing the person distress), there is a single victim, it has happened on two or more occasions and the victim is willing to report to the Police, under Section 7 of the Protection from Harassment Act 1997, the offender may be arrested. If it is the first time it has happened, but serious enough to warrant contacting the Police, it will be recorded as a first case harassment and a notice will be served on the offender to stop the activity causing the issue i.e. texting, phone calls etc. This will be recorded and the offender warned. If it happens again then they will be arrested.

Acceptable use policies

It is best practice for organisations to have clear and understood policies in place that include the acceptable use of technologies by service users and staff that address cyberbullying. Agreements on the responsible use of technology should include acceptable behaviour for service users, employees and volunteers, including behaviour outside of the organisation, for example use of social networking services and other sites, so as not to harm others or bring the organisation into disrepute.

Staff and volunteers should expect the organisation to react quickly to reported incidents or support the member of staff concerned to do so. It is also important that staff or volunteers who are harassed

in this way receive support and information enabling them to access appropriate personal support. The organisation should endeavour to approach internet providers or other agencies on their behalf in order to request that the inappropriate material is removed. The internet provider may only accept a request from the victim. However, the organisation may want to take action if it is on a work website or email address.

If it is necessary for the person being bullied to contact the service providers directly, the organisation may provide support. This might apply, for example, in cases of identity theft, impersonation or abuse via a mobile phone service.

Getting offensive content taken down

If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure they understand why the material is unacceptable or offensive and request they remove it.

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.

Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is; for example, by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected of being illegal you should contact the police directly.

More information can be found at:

https://www.gov.uk/workplace-bullying-and-harassment

http://www.saferinternet.org.uk/about/helpline

http://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation

https://www.getsafeonline.org/

https://www.ceop.police.uk/

http://safeguarding.dudley.gov.uk/

DMBC Staff:
https://connect.dudley.gov.uk/documents/_layouts/15/WopiFrame.aspx?sourcedoc=/documents/shared/Human-Resources/Bullying%20and%20Harassment%20Leaflet.doc&action=default&DefaultItemOpen=1

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. If you are being bullied they will help you to change your number if necessary. If you want to prosecute the perpetrator contact the police. The mobile provider will work closely with the police and can usually trace malicious calls for them.

Service providers: Service provider	**From your mobile**	**Pay as you go**	**Pay monthly contracts**
O2	4445 or 202	08705 678 678	0870 241 0202
VodaFone	191	03333 040 191	03333 048 069
3	333	08433 733 333	08433 733 333
EE	150	0800 956 6000	0800 956 6000
Orange	150	07973 100 450	07973 100 150
T-Mobile	150	07953 966 150	07953 966 150
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Dudley Safeguarding

protecting children, young people and adults at risk