Cyberbullying Guidance for Educational Settings

By effectively preventing and tackling bullying, educational settings can help to create safe, disciplined environments where pupils are able to learn and fulfil their potential. Oxfordshire County Council is committed to supporting settings in effectively preventing and tackling all forms of bullying, including cyberbullying. This document has been produced to help school leaders take effective action to prevent and respond to cyberbullying as part of their wider work to promote respectful relationships.

Glossary:

- **App -** an application, especially as downloaded by a user to a mobile device.
- **Cyberbullying** - the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
- **Cyber security** - is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.
- **Dark Web** - It is part of the World Wide Web that is only accessible through special software.
- **Deep Web** - it is part of the World Wide Web which is hidden from public view. The contents are not indexed by the usual search engines. It mainly consists of databases that can be made up of web mail and online banking, for example.

Guidance on cyberbullying:

- DfE Preventing and Tackling Bullying - July 2017
- OCC Anti-Bullying Template Policy – October 2020
- Childnet (as part of UK Safer Internet Centre) in-depth guidance - this guidance can be viewed or downloaded as a complete document or in sections.
- Cyberbullying guidance - summary leaflet
- Safe to learn - Embedding Anti-Bullying Work in Schools - cyberbullying
- Cyberbullying - Supporting School Staff - advice for school staff effected by bullying

Useful cyberbullying links:

- DfE Preventing and Tackling Bullying - Guidance for settings on preventing and responding to bullying.
- ChildLine – Information for young people on types of bullying from online bullying to racial, religious and homophobic bullying, plus tips on how to bounce back if they've been bullied.
- CEOP – If you're worried about online abuse or the way someone has been communicating online, let CEOP know.
- Thinkuknow - Thinkuknow is the education programme from NCA-CEOP, a UK organisation which protects children both online and offline.
- Internet Matters - Cyberbullying – Specialist advice for parents/carers and professionals on all online safety issues and parental controls.
- UK Safer Internet Centre - Best practices and resources for settings.
- Bullying UK - Information on all forms of bullying. This link takes you straight to information about cyberbullying, the effects of cyberbullying, how to deal with it and stay safe online.
- Kidscape - Advice for parents/carers, professionals and young people on all forms of bullying, including cyberbullying and digital safety.
- Anti-Bullying Pro - Advice from The Diana Award for parents/carers, professionals and young people on all forms of bullying, including cyberbullying.

- NSPCC - Advice for parents and carers to help keep children safe from bullying, wherever it happens.
- Stand Up to Bullying – A website dedicated to Stand Up To Bullying Day which aims to raise awareness of what bullying is, how it occurs and what to do about it.
- Anti-Bullying Alliance - Advice for parents/carers, professionals and young people on all forms of bullying. The Anti-Bullying Alliance also organise and produce resources for Anti-Bullying Week every year.

How should educational settings respond to cyberbullying concerns involving learners?

1. Reassure
Support the child being targeted and reassure them that they have done the right thing by reporting cyberbullying behaviour. Advise them how to deal with it appropriately (e.g. how to block bullies or report the users). Instruct them to keep evidence of cyberbullying by taking screen prints (including times, dates, names and locations if possible) or keeping messages. Stress the importance of not retaliating, and ensure they have access to support, if required.

Use existing pastoral systems and procedures to support the child(ren) involved and act as outlined in your Anti-Bullying Policy - this may involve speaking with the child's parents/carers or supporting them to do so themselves.

2. Respond
If possible, identify those who have caused harm and discuss the concern with them directly (with appropriate evidence, if possible). The setting should act in-line with the relevant policies (e.g. anti-bullying and behaviour). Consider how to change the behaviour/attitude of the harmer(s), think through appropriate use of restorative practice, education, sanctions and support. The incident (including action taken) should be logged as a cyberbullying incident and recorded in the anti-bullying and/or child protection records.

3. Remove/Report
Act to remove any harmful content. Contact service providers/Local Authority/Police, where relevant. In some cases, the quickest way to have content removed is for the person who posted it to remove it. If a criminal offence has been committed, seek assistance from the police via 101 (e.g. be mindful not to implicate yourself by viewing explicit images). For emergencies (e.g. if someone is injured, in danger or there is a risk to someone's life), contact 999.

4. Re-evaluate
Following any cyberbullying concerns, revisit policies, procedures and education approaches to identify if alternative action could prevent a future occurrence.

Whilst implementing lessons and assemblies in response to a cyberbullying concern can demonstrate a clear message to learners that cyberbullying will not be tolerated, it may not always result in a long-term behaviour change (no matter how “hard hitting” it is). Additionally, if there is a focus on shock or scare tactics (over practical and realistic advice), it can frighten children which may prevent them reporting concerns in the future.

For incidents that involve a small number of learners, consider 1:1 or small group work (such as restorative practices). Often there will be underlying issues such as unhealthy peer relationships and low esteem. In some cases, online safety specific advice isn’t required, and will be unsuccessful in the long-term if underlying issues are not explored and, where possible, resolved.

If appropriate, utilise Oxfordshire County Council's useful e-safety resources library to support your work to prevent recurrence.

What should educational settings do to prevent cyberbullying?

Settings should ensure there is a coordinated approach to bullying, including online bullying, so that all incidents are effectively managed to prevent recurrence.

Like any organisation, settings can also fall victim to a cyber-attack or incident. This can disrupt services and adversely affect the operation of an organisation and put members of the community at risk. For more information on effective cyber security, click on this National Cyber Security Centre link.

With cyberbullying and cyber security, the focus must always be on effective prevention and responses that reduce the likelihood of recurrence.

Recommended approaches for preventing and tackling cyberbullying:

- Settings must explicitly include cyberbullying in behaviour and anti-bullying policies and ensure that appropriate interventions are put in place and communicated to the whole community.
- Settings must ensure they have an up-to-date online safety policy and that the Designated Safeguarding Lead (DSL) works alongside other key members of staff to identify learners most vulnerable to such bullying.
- Settings must have Acceptable Use Policies (AUPs) which state the rules and expectations for all members of the community regarding online behaviour. It is important that they are understood and respected by staff, children and parents/carers - it is common practice for settings to insist that the AUP policy is signed to promote compliance and enable accountability.
- Every member of staff must understand what cyberbullying means, the different methods in which it can take place, the impact on those targeted and the setting's policies and procedures.
  - All members of the community should be aware of the 'Dark Web' and 'Deep Web'. For more information on the risks of the 'Dark Web' and 'Deep Web' and how to report concerns, visit this Internet Matters webpage.
- Settings must have a Staff Code of Conduct which states the expectations of all staff when they are communicating face-to-face and online, in and outside of the setting. Ensure staff are actively engaged in the online world and are role modelling positive online behaviour and communication.
- Senior leaders should ensure that they are aware of and managing the settings online reputation and consider ways in which to prevent concerns – e.g. see New advice for managing your school's online reputation.
- Senior and middle leaders should be aware of how to respond to online bullying issues, including where staff are the victims of online harassment.
- All staff should encourage children, young people, staff and families to be aware of their responsibilities in ensuring they use technology safely and responsibly – e.g. see Childnet's Family Agreement.
- All staff should educate children in how to keep themselves safe online, including responding to cyberbullying, by establishing an embedded and progressive online safety curriculum which is delivered creatively within and beyond the Computing Curriculum (e.g. through displays, assemblies, workshops, peer support, the student council, ad hoc interventions.)

- Engage with parents/carers about how they can help protect their children online – e.g. see Tips, advice, guides and resources to help keep your child safe online from UK Safer Internet Centre
- Use appropriate techniques to resolve the issues between those who bully and those who have been bullied. Oxfordshire County Council promote the use of Restorative Practice to prevent and tackle all forms of bullying. For more information, visit our Restorative Practice webpage or contact clare.pike@oxfordshire.gov.uk
- Regularly canvas children and young people's views on the extent and nature of online bullying – e.g. see NFER Young people and e-safety survey for example questions
- Have clear internal reporting procedures to support those targeted (e.g. Whisper Anonymous Reporting) and publicise the details of helplines and support websites/services.
- Challenge any behaviour or practice which does not uphold the values of tolerance (or acceptance), non-discrimination and respect towards others online – e.g. see Ofsted Inspection Framework (May 2019) - Parts 15, 16, 27 and 28.
- Proactively gather and record concerns and intelligence about bullying incidents and issues to effectively develop strategies to prevent bullying from occurring and recurring – e.g. on CPOMS, MyConcern, etc.
- Encourage children and their parents to raise concerns directly with the setting, for example, ensuring a senior member of staff is available on the gate at morning / afternoon pick up time, using dedicated email accounts for reporting issues.

How should educational settings respond to cyberbullying concerns involving staff?

Childnet and the DfE have guidance relating to these concerns.

Senior leaders of Oxfordshire schools may wish to contact the following places for advice regarding specific concerns relating to complaints or issues on social media sites:

- The Local Authority Designated Officer (LADO) if an allegation has been made against a member of staff
- The Professional Online Safety Helpline
- Thames Valley Police, if a criminal offence has been committed
- Their Union (many unions, including NAHT have specific advice regarding these issues)
- Should a setting or employing body require legal advice, Oxfordshire County Council offer legal support as a traded service. For more information on how to access Legal Services, go to: https://schools.oxfordshire.gov.uk/cms/content/legal-services

Advice to share with staff to help protect them from cyberbullying:

- Keep all passwords and login details secret from pupils, friends, family and colleagues and make sure you understand how to secure any websites or social networking services.
- Always think carefully before you post - don't post any information (e.g. photos, videos and comments) online that you wouldn't want employers, colleagues, pupils or parents to see.
- Keep any personal devices such as mobile phones secure (ideally switched off) whilst at work. Make sure you understand how your device works and which features could make you vulnerable (e.g. keep your Bluetooth switched off or hidden). Your setting will likely have a policy on mobile phone use so follow this.
- Be aware that just because your profile is set to "Private" or "Friends Only", it doesn't mean that someone else can't copy or share it without your knowledge.

- Manage your digital reputation. Always consider if content posted online could bring you, your setting or someone else's reputation into disrepute.
- The Teacher's standards is clear that teachers should not bring the profession or institution into disrepute, this includes through conduct online. Posting something unsafe, inappropriate, obscene or threatening online could lead to criminal, civil and/or disciplinary action.
- Staff must not add or 'friend' pupils (past or present) or their parents/carers on any personal social networking accounts. Discuss any issues or exceptions with this (for example any pre-existing relationships) with your headteacher/manager or the setting's Designated Safeguarding Lead (DSL). Guidance on this should be available via your Staff Code of Conduct and Acceptable Use Policy.
- Keep all personal information (phone numbers, email addresses, locations) private.
- Do not use your own personal devices or personal social networking profiles to contact pupils or parents/carers. Communication with pupils/families and colleagues should always be professional, transparent and open to scrutiny and should therefore take place via official communication channels or using official equipment.
- Ensure that the setting's rules and policies regarding the use of technologies by pupils and staff are enforced. Make sure you read and understand the setting's online safety policy and procedures.
- Always report any incidents of online bullying of staff to the headteacher and website/service provider, in a timely manner.
    - Do not personally retaliate to any incidents which involve yourself or other members of staff.
    - Make sure you save and keep any evidence of bullying, e.g. screen prints to show your line manager and/or the police. Where possible, record times, dates and usernames.
    - Check with your union to see if they offer any guidance or support about online bullying and professional behaviour online.
- Staff and leaders working in Oxfordshire educational settings can access specific support and advice regarding online bullying via the Education Safeguarding Advisory Team and the Professional Online Safety Helpline.

Feedback

Online feedback form

Last updated 16th October 2020