Cyberbullying Policy and Procedure

Agreed by Governing Body: Autumn 2019
To be reviewed: Autumn 2021
Group Responsible: Full Governors

Contents

(Click on the headings below to jump to the relevant section)

Introduction

Cyberbullying is a form of harassment using information and communications technology (ICT), particularly; mobile phones, social media and internet, with the purpose of trying to deliberately upset, threaten and intimidate someone else. It is a "method" rather than a "type" of bullying and includes bullying via messaging, instant messenger services, social network sites, email, images and videos posted on the internet or spread by mobile phone. Cyberbullying can take the form of 'cyber-stalking' (e.g. repeatedly messaging an individual), exclusion/isolation, sexting (e.g. sending sexually explicit messages), impersonation, defamation, publication of private information/images without consent and 'trolling' (e.g. making random unsolicited and/or controversial comments on social media/internet forums with the intent to provoke an emotional knee-jerk reaction from unsuspecting individuals to engage in a fight or argument).

Harassment occurs when one person pursues an unwanted course of action to another that violates that person's dignity and causes them alarm or distress. Individuals can be reluctant to admit being a victim of cyberbullying. Any incidents of cyberbullying should be taken very seriously, and employees should always feel encouraged to report any incidents that occur.

Increasingly there are legal cases about staff being bullied or victimised, through sustained inappropriate posts (either personally or professionally) on social media. These posts are sometimes from parents but also increasingly from pupils who are critical of an individual within a school or the school itself.

Policy statement

This school does not tolerate any form of bullying or harassment. This policy relates to cyberbullying and is part of the suite of policies and procedures related to bullying and harassment. This school is committed to protecting the safety and well-being of its staff from online activities that are harmful and damaging and which can, in some circumstances, constitute a criminal act. This could include unlawful harassment as well as mental and physical injury at work.

Any complaints from staff who feel they have experienced cyberbullying will be taken very seriously, dealt with promptly, fairly and where appropriate dealt with as a disciplinary offence.

This policy is informed by the non-statutory guidance; 'Cyberbullying: Advice for Headteachers and schools staff' and; Searching, screening and confiscation: advice for schools and the statutory guidance 'Keeping Children Safe in Education'. All published by the DfE.

Scope

This policy and procedure forms part of the school's overall commitment to anti-bullying. It applies to all employees of the school.

1. Relevant legislation

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. There is no specific cyberbullying law but cyberbullying, or actions related to cyberbullying, could be an offence under any of the below:

- Equalities Act 2010 – protection against discrimination, harassment or victimisation
- The Education and Inspections Act 2006 (maintained schools only – see section 7.2)
- The Education (Independent Schools Standards) (England) (Amendment) Regulations 2012 (Duty on academies to have an effective anti-bullying strategy and to comply with Health and Safety Law).
- Management of Health and Safety at Work 1999 - provision of health surveillance where identified by risk assessment
- Health and Safety at Work Act 1974
- Protection from Harassment Act 1979
- Defamation Act 2013
- The Malicious Communications Act 1998
- Data Protection Act 2018
- Communications Act (2003)
- Obscene Publications Act (1959)
- Computer Misuse Act (1990)

2. Related school policies and procedures

This policy should be read and operated in conjunction with the following policies:

- Internet, social networking and email use policy
- Bullying and Harassment policy
- Grievance procedure
- Disciplinary procedure

- Code of conduct
- Safeguarding policy
- Incident reporting policy
- Violence at work policy
- Online safety policy
- Acceptable use policy (ICT)
- Anti-bullying policy

3. Employees responsibilities

Employees are expected to act in a professional manner at all times and take steps to protect their online reputation. Employees:

- should feel safe and encouraged to report any incidents of cyberbullying immediately (see section 5 for how to report).
- should ensure they understand their school's policies on the use of social media.
- must not leave a computer or any other device logged in when they are away from their desk.
- should enable a PIN or passcode on their mobile phone. This is an important step to protect them from losing personal data and images (or having them copied and shared) from their mobile phone or device if it is lost, stolen, or accessed by pupils.
- should familiarise themselves with the privacy and security settings of the social media and
  apps they use and ensure they are kept up to date.
- should keep a check on their online presence – for example by typing their name into a search engine. If there is negative content online, it is much easier to deal with this as soon as it appears.
- should be aware that their reputation could be harmed by what others share about them online, such as friends tagging them in inappropriate posts, photographs, or videos.
- should consider their own conduct online; certain behaviour could breach their employment code of conduct. See the school's Disciplinary policy.
- should discuss these same issues with close family, friends and colleagues, as they could become a target if they do not have security and privacy settings in place.
- should not accept friend requests from pupils past or present. If they feel this is necessary, they should first seek guidance from a senior manager.
- should be aware that their social media friends may also be friends with pupils and their family members and therefore could read their post if they do not have appropriate privacy settings.
- should not give out personal contact details – if pupils need to contact employees regarding homework or exams, they should always use the school's contact details.
- should have a school mobile phone rather than having to rely on their own, when on school trips
- must use their school email address for school business and personal email address for their private life; and must not mix the two. This includes file sharing sites; for example, Dropbox and YouTube.

- must read the policies outlined in section 2.

4. School responsibilities

Bullying is not tolerated in any form. The best way to deal with cyberbullying is to prevent it happening at all. The school will:-

- have in place appropriate policies and strategies to prevent bullying and harassment, discrimination and victimisation
- have appropriate support mechanisms in place to support employees experiencing cyberbullying.
- provide health surveillance where there is an identifiable work-related condition, there is a likelihood of recurrence, or where surveillance will help protection.
- will make sure that parents and carers are aware and understand how to communicate with the school so that if a situation arises the appropriate reporting procedures are known and clear.
- Record and investigate all complaints by staff of cyberbullying swiftly and fairly.

5. Procedure/Management action

5.1 Cyberbullying of staff is not acceptable. If an employee feels they are a victim of cyberbullying they should do the following:

- never respond or retaliate.
- report it to the Headteacher and seek support from them or a senior member of staff.
- Norfolk Support Line provides a 24/7 counselling service, which can provide support in this type of situation.
- if you are a trade union member, contact your Trade Union for support
- if possible, save evidence of the abuse – screen shots and record the time and date
- if the comments are threatening, abusive, sexist, of a sexual nature or constitute a hate crime consider calling the police - 999 in an emergency or 101 in a non-emergency situation. Reports can also be made online to the police.

5.2 As soon as a complaint is made, support should be offered to the employee and evidence should be gathered immediately, including the harm caused. Any adverse comments from parents of existing or prospective pupils should be logged, particularly when they result in the withdrawal of a pupil from the school or a decision not to proceed with a job or admissions application.

5.3 The Headteacher and the employee should agree on the course of action to be taken. This will usually mean informing the individual in question that their behaviour, in harassing a school employee, was unacceptable and try to re-build the relationship. Where the individual is a pupil or colleague, the majority of cases

can be dealt with most effectively through the school's own mediation or disciplinary procedures.

5.4 If employees or managers need to seek advice about inappropriate use they can speak to their HR provider or contact the Online Safety Helpline (email: helpline@saferinternet.org.uk or call 0344 3814772). However, employees and managers should not bypass the school's safeguarding procedures.

5.5 Parents

5.5.1 If a parent/guardian makes inappropriate comments about a member of staff on social media the school should take appropriate action. As a first step the employee(s) in question should be offered support as the situation is likely to cause distress. They should be advised not to respond to the post(s) on social media.

5.5.2 The school should have a discussion/meeting with the parent, which could include advice on available routes for concerns; discussion of a resolution to the concern and request to remove the information. To request that abusive materials are taken down, a Headteacher should meet with the parent(s) involved. In this type of meeting, the headteacher should:

- address the matter of social networking with them and explain how this behaviour can have a detrimental impact on the school and potentially their children's education while not allowing the school to actually address their concerns.
- ensure parents are aware that comments posted online (even if made 'privately') can easily be misinterpreted and shared without their knowledge or consent
- ensure printouts of the allegations or comments are available
- stress that the school may have to take further action, including criminal proceedings where illegal content is involved, to resolve the matter if the meeting is unsuccessful.
- if the individual has a reasonable complaint they should be informed of the correct school procedure for making a complaint.

5.5.3 Reaching a solution in meetings with the member of the public may be very difficult. In some situations, it may be advisable to have a second meeting with a Governor to resolve the situation or to use a trained mediator.

5.5.4 If the meetings prove unsuccessful, headteachers could then send a letter to the parent requesting that the parent does not visit the school premises unless invited to attend an appointment, such as parents' evening.

5.5.5 In the situation where a parent or carer has harassed a teacher, further action would normally take the form of a letter from the Headteacher to the individual. The letter would underline the fact that it is not acceptable behaviour to harass a school employee, and if the individual wishes to discuss the matter further arrangements

for this can be made. The subsequent meeting should take place in the presence of the Headteacher and a Governor.

5.6 Pupils

The Education and Inspections Act 2006 gives schools the power to:

- regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff;
- confiscate items from pupils, including mobile phones, when they are being used to cause a disturbance in class or contravene behaviour or anti-bullying policies or used to commit an offence;
- request a pupil to reveal a message or show other content on their phone for the purpose of establishing if bullying has occurred;
- where the school's behaviour policy expressly provides, search through a phone where a pupil is reasonably suspected of involvement.

The above must be read in conjunction with section 5.3 of this policy, the school's Anti-bullying/Cyberbullying policy for pupils and 'Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies' published by the DfE.

While these powers may not offer an immediate remedy, they do at least provide schools with the means to discipline pupils suspected of cyberbullying.

5.7 Other staff members

The school's Bullying and Harassment policy will be followed. It may be necessary for disciplinary action to be taken.

5.8 Where there are repeated cases of harassment by the same individual the Headteacher should undertake a risk assessment.

5.9 Where the complaint is deemed to be harassment the school's Dignity at Work procedure should be followed (procedure for harassment by external parties where applicable).

5.10 Where the cyberbullying has taken place on a social networking site and the posts have breached the terms of the site, the school should contact the host/provider of the site to ask for removal – see the DfE cyberbullying guidance for further advice.

6 Employer liability for the actions of parents, pupils or staff who cyberbully

6.1 Schools will be liable for failing to take steps against pupils who subject teachers to discriminatory bullying and harassment where the 'reason' for failing to act is itself discriminatory e.g. a school has taken steps in the past against pupils who racially abuse staff, but has failed to take steps where pupils subject employees to

homophobic bullying as the individual on the receiving end of the bullying could claim that they have been treated less favourably.

6.2 The Equality Act 2010 (Section 40) makes an employer liable for the acts of a third party i.e. a pupil or parent, where the employer knows that the employee has been subjected to harassment by third parties (but not necessarily the same third parties) on two separate occasions and has failed to take 'reasonably practicable' steps to prevent the harassment from recurring.

7. Monitoring of electronic activity

Where the school believe unauthorised use of the information systems may be taking place, or the system may be being used for criminal purposes, then the decision may be taken to monitor an employee's use of the school's information systems. Additionally, schools can check social networking sites where an employee has reported an instance of cyberbullying. However, whilst the school has the right to monitor electronic activity they must balance this with the employee's human right to privacy. The school's Internet, social networking and email use policy details further information on monitoring and how to undertake it legally and appropriately.

8. Data Protection

When dealing with cyberbullying complaints the school processes personal data collected in accordance with its data protection policy. Data collected by the school as part of a cyberbullying complaint is held securely and accessed by, and disclosed to, individuals only for the purposes of dealing with the complaint. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the school's data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the school's disciplinary procedure.

9. Other resources

Childnet's 'Using Technology' guide
The UK Safer Internet Centres Reputation

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
14/05/2019	2, 5.7, 5.9	References to Dignity at work policy updated to Bullying and Harassment policy.
21/08/2018	All	New policy