Cyberbullying policy and procedure

Formally adopted by the Governing Board of:-	**Caister Primary Federation**
On:-	**January 2026**
Chair of Governors:-	**Payal Patel**
Last updated:-	**May 2024**

Cyberbullying policy and procedure P319a

Contents

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

1. Introduction and scope 2
2. Equalities and support 3
3. Relevant legislation 3
4. Related school policies and procedures 3
5. Employees responsibilities 4
6. Governing Board responsibilities 5
7. Procedure 5
8. Management action 5
9. Parents 5
10. Pupils 6
11. Other employees 7
12. Employer liability for the actions of parents, pupils or employees who cyberbully 7
13. Monitoring of electronic activity 7
14. Data Protection 7

Appendix 1 – Table of changes 8

We, the Governing Board, have adopted this policy and procedure.

1. Introduction and scope

1.1 This policy and procedure forms part of our overall commitment to anti-bullying. It applies to all employees. There is a separate policy for pupils.

1.2 We do not tolerate any form of discrimination, bullying or harassment. This policy and procedure specifically relates to cyberbullying and is part of the suite of policies and procedures related to discrimination, bullying and harassment.

1.3 We are committed to protecting the safety and well-being of our employees 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.

1.4 Cyberbullying is a form of bullying or harassment using electronic media and information technology with the purpose of trying to deliberately embarrass, upset, threaten, intimidate or target another person. 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).

1.5 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 will be taken very seriously, and employees should always feel encouraged to report any incidents that occur.

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

1.7 Throughout this policy the word "parent" should be read as inclusive of carers and any other person with parental responsibility.

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

1.9 This policy is informed by the non-statutory DfE guidance; 'Cyberbullying: Advice for Head of School s and schools staff' and; Searching, Screening and Confiscation: advice for schools and the statutory guidance 'Keeping Children Safe in Education'.

2. Equalities and support

2.1 The Head of School will ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless of age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; or sexual orientation.

2.2 Through the implementation of this policy and procedure, the Governing Board will be mindful of their obligation to seek to maintain and protect the mental health and wellbeing of all employees as far as is reasonably practicable.

2.3 According to ACAS it is estimated one in seven people are neurodivergent, meaning that the brain functions, learns and processes information uniquely. Where an employee discloses neurodiversity, the Governing Board understands the employee may require extra support in relation to the application of this policy. Where reasonable adjustments are necessary and can be accommodated, the Head of School will support these.

3. Relevant legislation

There is no specific cyberbullying law or legislation, but cyberbullying, or actions related to cyberbullying, could be an offence under various legislation including (but not limited to):

- The Equalities Act 2010 – protection against discrimination, harassment or victimisation
- The Education and Inspections Act 2006 (for maintained schools only)
- The Education (Independent Schools Standards) (England) (Amendment) Regulations 2012 (places a duty on academies to have an effective anti-bullying strategy and to comply with Health and Safety Law).
- Health and Safety at Work Act 1974
- Protection from Harassment Act 1979
- Defamation Act 2013
- Malicious Communications Act 1998

4. Related school policies and procedures

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

- Social media and electronic communications policy
- Discrimination, 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

5. Employees responsibilities

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

- should feel safe and are encouraged to report any incidents of cyberbullying immediately (see section 7).
- should ensure they understand the 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 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 4.

Further information on using technology can be read on childnet.com, along with understanding and managing your online reputation on UK Safer Internet Centre.

6. Governing Board responsibilities

The Governing Board will:-

- have in place appropriate policies and strategies to prevent discrimination, bullying, harassment and victimisation.
- have in place a member of staff or team to lead on anti-bullying, including cyberbullying of employees.
- 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.
- 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 employees of cyberbullying swiftly and fairly.

7. Procedure

7.1 If an employee feels they are a victim of cyberbullying they should:

- never respond or retaliate.
- report it to **the Head of School** and seek support from them or a senior member of staff.
- contact their Trade Union for support if they are a member.
- save evidence of the abuse, if possible, by using screen shots and recording dates and times.
- consider calling the Police (by dialling 999 in an emergency or 101 in a no-emergency situation) if the comments are threatening, abusive, sexist, of a sexual nature or constitute a hate crime. Reports can also be made online to the police.

8. Management action

8.1 As soon as a complaint is made, support should be offered to the employee and evidence should be gathered immediately, including the harm caused.

8.2 The Head of School and the employee should agree on the course of action to be taken. This will usually mean informing the perpetrator that their behaviour is unacceptable and trying to re-build the relationship. Where the individual is a pupil or colleague, the majority of cases can be dealt with most effectively through mediation or disciplinary procedures.

8.3 If employees or managers need to seek advice about inappropriate behaviour, they can speak to their HR provider or contact the Online Safety Helpline by emailing helpline@saferinternet.org.uk or by telephone on 0344 3814772). However, employees and managers should not bypass the school's safeguarding procedures.

9. Parents

9.1 Any adverse comments from parents of existing or prospective pupils should be logged.

9.2 Where the complaint is deemed to be harassment, the Discrimination, bullying and harassment policy should be followed (Appendix A – Complaints of harassment by external parties).

9.3 If a parent makes inappropriate comments about an employee on social media, the Head of School will take appropriate action. As a first step, the employee(s) should be offered support as the situation is likely to cause distress and they should be advised not to respond.

9.4 The Head of 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.

9.5 When requesting that abusive materials are taken down, the Head of School will meet with the parent(s) involved. In this type of meeting, the Head of School 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 child's education while not allowing the school to 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 Governing Board may have to take further action, including criminal proceedings where illegal content is involved, to resolve the matter if the meeting is unsuccessful.
- inform the parent of the correct procedure for making a complaint if they have a reasonable complaint.

9.6 Reaching a solution in meetings with the parent 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.

9.7 If the meetings prove unsuccessful, the Head of School is advised to 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.

9.8 In the situation where a parent has harassed an employee, further action would normally take the form of a letter from the Head of School to the parent. The letter would underline the fact that it is not acceptable behaviour to harass an 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 Head of School and a Governor.

10. Pupils

10.1 Current statute gives schools the power to:

- regulate the conduct of pupils when they are off-site or not under the control or charge of an employee.
- 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.
- search through a phone where a pupil is reasonably suspected of involvement, where the school's behaviour policy expressly provides.

10.2 The DfE's Searching, screening and confiscation: guidance for schools on gov.uk summarises the powers available to schools under the statute.

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

11. Other employees

11.1 Where the perpetrator is another employee, the Discrimination, bullying and harassment policy will be followed. It may be necessary for disciplinary action to be taken.

11.2 Where there are repeated cases of harassment by the same individual, the Head of School will need to determine an appropriate plan of action to deal with the harasser and to protect the harassed.

11.3 Where the incident is deemed to meet the Violence at work compliance code, an incident reporting form should be completed on the incident reporting system.

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

12. Employer liability for the actions of parents, pupils or employees who cyberbully

12.1 The Governing Board will be liable for failing to take steps against pupils who subject employees 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 employees but has failed to take steps where pupils subject employees to homophobic bullying as the employee could claim that they have been treated less favourably.

12.2 The Equality Act 2010 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) and has failed to take 'reasonably practicable' steps to prevent the harassment from recurring.

13. Monitoring of electronic activity

13.1 Where it is believed 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, social networking sites can be checked where an employee has reported an instance of cyberbullying. However, whilst the Head of School has the right to monitor electronic activity, they must balance this with the employee's human right to privacy. The social media and electronic communications policy details further information on monitoring and how to undertake it legally and appropriately.

14. Data Protection

Personal data collected and processed for the purpose of this policy and procedure will be handled in accordance with the data protection policy and applicable statutory obligations. Any personal data collected is held securely and accessed by, and disclosed to, individuals only for the purposes of employee management or to comply with statutory reporting obligations. Inappropriate access to, or disclosure of, employee data constitutes a data breach and should be reported without delay, in accordance with the data protection policy. It may also constitute a disciplinary offence in which case it would be dealt with under the disciplinary policy and procedure.

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
14.01.2026	Whole document	Parent/Carer added in place of parent only
14.01.2026	1.8	Confidentially added
14.01.2026	4	The word applied added after read and
14.01.2026	8.1	Details of any harm added
11/02/2025	All	Review of whole document and terminology to ensure consistency across all policies and procedures.
10/07/2023	10	Updated reference to Internet, social media and email use model policy P319 to Social media and electronic communications model policy P319.
16/11/2021	2	Additional paragraph to include consideration for employees with mental health issues.
24/06/2020	5.9	Reference to dignity at work procedure updated to Bullying and Harassment policy
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