

ANTI-CYBERBULLYING POLICY

Any form of bullying, whether verbal, physical or psychological, is completely unacceptable at Sherborne International.

The purpose of this policy document is to enable the School to provide a clear understanding about the School's attitudes to cyber-bullying, about the action which will be taken to prevent it happening, and the School's response, and legal position if it should occur. It should be read in conjunction with the School's E-Safety Policy.

Cyberbullying can be defined as *'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.'*

Cyberbullying can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying:

- the invasion of home and personal space at any time of day or night
- the difficulty in controlling electronically circulated messages
- the size of the audience
- perceived anonymity
- the profile of the person doing the bullying and their target

Cyberbullying is a specific form of bullying which is increasing in prevalence and is unique in its potential to involve staff, as well as students, in being bullied by individuals.

It is also unique in that acts of cyberbullying, whilst not a specific criminal offence, may involve the breaking of UK laws regarding harassment and threatening communications. Dealing with acts of cyberbullying could therefore result in the involvement of the police.

Forms which cyberbullying may take:

- threats and intimidation
- harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages)
- vilification / defamation
- exclusion or peer rejection
- impersonation
- unauthorised publication of private information or images (such as in response to 'sexting' events)
- manipulation or grooming

It is important to recognise that not all apparent cases of cyberbullying are deliberate or aggressive, but may be the result of unthinking acts in which images or comments are shared in the belief that they are amusing without any realisation of the distress caused. In addition, since groups of pupils may be involved, each message quickly builds to give a persistent bullying pattern. These instances are to be treated seriously but not necessarily with the same severity as obviously intentional acts of cyberbullying.

Prevention of cyberbullying

Staff will talk with students to understand the ways in which they are using the internet and mobile phones and will give guidance on how students can guard against becoming the target of cyberbullying, or even carrying out acts which may result in the student being accused of cyberbullying.

Students are not given access to the School's internet facilities before they have signed the School's Acceptable Usage Policy which asks parents to explain the policy to their child. The AUP is explained to students to ensure they have a good understanding of its requirements, including safe and appropriate use of the internet, the need to report any cases of cyber-bullying and to ensure that they do not become a cyber-

bully themselves, even inadvertently. Due to the fact that all our pupils speak English as an additional language, a shortened version of the AUP, written in simple English, is carefully explained and signed by each child in their first ICT lesson.

The School has a dedicated E-Safety Officer who leads a Digital Council (whose members are part of the student body). It also has a robust E-Safety Policy which details roles and responsibilities, use of technology in the classroom and online safety.

The School conducts regular reviews and audits of the safety and security of school ICT systems and provides enhanced user-level filtering through the use of the school's multi-language filtering programme, which is monitored by the Systems Manager. Staff have a duty to report to the E-Safety Officer and Systems Manager anything they believe may be a potential loophole in the School's internet filtering system. Server records are checked regularly for attempts to access inappropriate material and such issues are taken forward by the Vice Principal and E-safety Officer as appropriate.

Education on cyberbullying and its effects is delivered concurrent with education on other forms of bullying (*see anti-bullying policy*). Students also receive specific education on the safe use of technology and the implications of posting personal information online throughout their time in School. This education is delivered through a variety of routes, including PSHE, tutorials, lessons, assemblies, development seminars led by external agents, and through boarding life. Staff also receive training regarding online safety delivered by Karl Hopwood, an external expert.

Reporting of cyberbullying

Students will be encouraged to report instances of cyberbullying by the methods already outlined (*see anti-bullying policy*). Staff will also be vigilant for behaviours which may signal that a student is being bullied in this specific manner, such as:

- Being obviously upset after receiving a text message.
- Being unwilling to use computers or specific sites of prior interest.
- Being unwilling to discuss their mobile phone or internet use.
- Suddenly changing patterns of use of specific technologies.

Investigation of cyberbullying

If a student reports instances of cyberbullying, they will be encouraged to keep any evidence and provide it to staff. Evidence may take the following forms:

- Text messages or images saved on the recipient's phone.
- Posts on social networking sites.
- Websites created about an individual or in an individual's name.
- Threads on discussion boards.
- If the child reports an image that is explicit/obscene, **do not view the image**, but ask them to give a brief description. Tell the child **not to forward this image nor delete it**. Report this immediately to the **Designated Safeguarding Lead** (Mr Daryl Barker) or one of his Deputies (the Principal or Vice-Principal), who may seek the advice of the Local Safeguarding Children's Board or the Police.

Staff investigating instances of cyberbullying should proceed in line with the School anti-bullying policy, but should aim to gather evidence in the form of screen prints from websites, printouts of emails and transcripts of text messages. Images sent by text message will be recovered where possible and hard copies made.

If students are accused of sending upsetting texts, which the recipient has deleted, staff may ask to look at the perpetrator's phone for evidence if there is a reasonable suspicion that such texts have been sent. Staff may **not**, however, search a phone for information without the specific permission of its owner, and are

advised that any such search should be limited to students showing the investigating member of staff their phone messages themselves. Mobile phones may be confiscated from students if there is reasonable suspicion of use for the purposes of cyberbullying.

Staff should at all times be sensitive to the feelings of the bullied individual, who may find the evidence retrieved to be upsetting or very embarrassing. Students should be assured of discretion in dealing with such material as part of the upsetting nature of cyberbullying is the perception that 'everyone' is aware of such images or upsetting text.

If the electronic comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, the Designated Safeguarding Lead or his Deputies will take advice from the Local Authority's Designated Officer as to whether this reaches the threshold to be referred to the Dorset MASH team.

Any evidence generated in this manner will, upon resolution of the incident, be placed in an envelope on the students' file marked 'confidential'.

Action to be taken

If it is clear that acts of cyberbullying have taken place, the steps taken will be in line with the School anti-bullying policy but may also include:

- Asking the perpetrator to remove upsetting material from message boards, websites or computers and mobile phones.
- Contacting the service provider or host to request that material is removed.
- Contacting the nuisance call department of the victim's mobile phone provider to ask for certain numbers to be blocked.
- Blocking certain email addresses from reaching the victim and educating the victim on how to block individuals from accessing their pages on social networking sites.
- In line with the School's agreement with the student (the signed Acceptable Usage Policy) the School may suspend internet access for the perpetrator for a period of time.
- Contacting the parents of the perpetrator to inform them of the nature of acts carried out.

The **Education and Inspections Act 2006** (EIA 2006) outlines some legal powers which relate to cyberbullying. Head teachers have the power "to such extent as is reasonable" to regulate the conduct of students when they are off-site or not under the control or charge of a member of staff. This is of particular significance to cyber-bullying, which is often likely to take place out of School but which can impact very strongly on the school life of those students involved.

In serious cases of cyberbullying, as with bullying of other forms, the School reserves the right to apply more severe punishments (*see anti-bullying policy*).

If evidence appears to show that a student or another child is at significant risk of harm, the Designated Safeguarding Lead will be notified and the School safeguarding procedures will be followed (*see safeguarding policy*).

Legal implications

As discussed at the start of the policy, there are legal implications to acts of cyberbullying since the creation of images and text about individuals may cross into laws relating to harassment and the creation of indecent images. In the event of this being the case, the School reserves the right to seek legal advice and contact the police as necessary.

Cyberbullying and Staff

One of the characteristics of cyberbullying is that it has the potential, by its anonymity, to affect staff as they may become the target of acts of cyberbullying. The perpetrator may not be older or in a position of authority in order to bully an individual. Staff therefore have a responsibility to protect themselves from cyberbullying as far as possible and a right to support from School should an instance of bullying become apparent.

Staff should adhere to the guidelines contained in School's *Staff Code of Conduct*. The following guidance is also provided by the DSCF (*Cyberbullying: Supporting Staff*):

Images and video

- Staff should seek permission before sharing images of students online.
- Staff should be wary of allowing themselves to be photographed or videoed in unusual situations, however innocent they may seem, as these images could be used to ridicule or humiliate the subject at any point in the future.
- Significant information should not be attached to any images posted, such as full names, unless informed or parental consent has been obtained in advance.
- Any picture which causes distress to an individual, for any reason, should be removed straight away.

Mobile Phones

- Staff should be aware at all times of the increasing sophistication of mobile phones and their use in capturing information and uploading content to the internet.
- Staff should take good care of their own phones at all times due to the amount of sensitive information they now contain. Phones should never be left unattended and should be locked with a security code when not in use.
- Staff should report, and have blocked, a missing phone straight away. To this end all staff should be aware of their phone IMEI number (printed on the phone underneath the battery or found by typing *#06# into the handset).
- Staff should avoid lending mobile phones to students if at all possible – even in an emergency. It would be more prudent to make the call for the student. However, if a personal mobile phone has to be lent to a student, the call should be supervised at all times and any numbers used deleted from the phone straight away.
- Staff should not give students or parents their personal mobile phone number (or personal email address). If a member of staff believes students or parents have obtained and are abusing either their personal mobile phone number or personal email address, these contact details should be changed and kept confidential.
- Staff should follow School guidelines on the possession of student's mobile phone numbers – see House manuals under 'Valuables and Other Personal Belongings', which informs students that the School will register their mobile telephones and log the numbers. This is to identify lost or disputed phones and enable the School to contact students directly if necessary (eg on an outing).

Social Networking Sites

- Staff should be mindful of how they present information about themselves on the internet, particularly in relation to images and personal information to which anyone could gain access and use inappropriately.
- Staff using such sites should ensure that they are aware of how to restrict access to their information online on the sites they use. In cases of uncertainty, staff are advised to treat all information as accessible to the public.
- Staff should not befriend current students on social networking sites and should be aware, if befriending ex-students, of the relationships which may exist between current and ex-students and

how this may potentially allow current students to access personal information. See also 'Social Media Policy' in the Staff Manual.

- For the same reasons, staff are advised not to befriend parents of students.
- Staff should occasionally use search engines to check what information is available about them in the public domain. Action in the case of cyberbullying.

If a member of staff believes they are being cyber-bullied, they should take the following steps:

- Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents or any other unusual or negative communication from students or parents. They should report incidents appropriately and seek support from a senior member of staff such as the Senior Housemaster or other senior member of the boarding staff. They may refer the incident to the Principal/Vice Principal who will discuss action with the member of staff, and the Systems Manager, if appropriate.
- Keep any records of the abuse – text, emails, voice mail, web site or instant message. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.
- Staff are advised that if they receive a message with any attachment which they believe to contain offensive or obscene content, they should not open the attachment but alert a senior member of staff.
- Where the perpetrator is known to be a current student or co-worker, the majority of cases will be dealt with by the School's own disciplinary procedures, with the involvement of other agencies in severe cases.
- There have been cyberbullying incidents where students have made unfounded, malicious claims against staff members. It is critical to take every claim seriously and investigate it thoroughly. In cases where an allegation is made that an employee or volunteer has behaved in a way that has harmed or may have harmed a child, possibly committed a criminal offence against or related to a child, or behaved towards a child or children in a way that indicates s/he is unsuitable to work with children then that allegation should be reported to the Principal immediately. This will then be investigated as outlined in the Safeguarding policy.

Summary of Key Advice for Staff:

1. Be aware, a student may as likely cyber bully as be a target of cyber bullying.
2. Be alert to a student seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. Please also note they might be particularly unwilling to talk, or be secretive about online or mobile phone problems.
3. Talk with students and understand the ways in which they are using the internet and their mobile phone. Frequently discuss the guidelines as provided to students in the student manual.
4. Report any potential loophole in the School filtering system to the E-Safety Officer and Systems Manager.
5. Remind students not to retaliate.
6. Keep the evidence of offending emails, text messages or online conversations and pass them on to the Vice Principal, Housemistress or Junior Housemaster.
7. Report cyber bullying or suspected cyber bullying at all times.

References:

Cyberbullying: Supporting School staff (DCSF, 2009)

Cyberbullying Safe to learn: Embedding anti-bullying work in schools (DCSF, 2009)



Preventing and Tackling Bullying (DfE 2017)

Cyberbullying: Advice for headteachers and school staff (2014)

Original policy written by Sue Shaw, January 2012

Reviewed by Mr I Elliott (ICSS Governor), Nov 2012

Reviewed and adapted for Sherborne International by SJB, January 2014; checked by PAH, June 2014; approved by MA, Sept 2014

Reviewed and revised by SJB, September 2015

Reviewed and revised by SJB, checked by PAH, August 2016

Reviewed and minor revision by AEH, September 2017

Reviewed by AEH, September 2018