CYBER BULLYING POLICY

INTRODUCTION

1. This policy is a 'Whole School Policy' and informs practice is the Senior School, Prep School and Nursery. Battle Abbey School recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the School community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

1.1 This policy should be read in conjunction with the following:

- Safeguarding and Child protection policy
- Anti-bullying Policy
- Social Media Policy
- ICT Policy

2. Bullying of any kind is unacceptable at Battle Abbey School; if cyber bullying harassment does occur, all pupils should be able to tell and know that incidents will be dealt with promptly and effectively. The School has a duty to protect all members of its community and provide a safe, healthy environment. The Head has the power 'to such extent as is reasonable' to regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff (Education and Inspections Act 2006); in other words, this policy applies both in and out of school. School staff may request a pupil to reveal a message or other phone content and may confiscate a phone; however, they may not search the contents of the phone without the permission of the pupil. Some cyber bullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997 (see below).

AIMS

3. The aims of this policy are to ensure that:

- Pupils, staff and parents are educated to understand what cyber bullying is and what its consequences can be.
- Knowledge, policies and procedures are in place to prevent incidents of cyber bullying in School or within the boarding community.
- There are effective measures to deal effectively with cases of cyber bullying.
- The effectiveness of prevention measures is monitored.

WHAT IS CYBER BULLYING?

4. Cyber bullying is the use of ICT, commonly a mobile phone or the internet, deliberately to upset someone else. It can be used to carry out all the different types of bullying; an extension of face-to-face bullying. It can also go further in that it can invade home/personal space and can involve a greater number of people. It can take place across age groups and School staff and other adults can be targeted. It includes threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images; and manipulation. Further information is at Appendix 1.

WHAT DOES UK LEGISLATION SAY?

5. Under UK legislation, cyber bullying can be considered a criminal offence under the following legislation:

- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1988
- Communications Act 2003
- Defamation Act 2013

In addition, under Section 1(1) of the Protection of Children Act 1978, it is a criminal offence deliberately and/or knowingly to either make, take, or permit to be taken, distributed or showed indecent photographs of children. Anyone using indecent, sexualised photographs of children as a part of cyber-bullying can be prosecuted.

PREVENTING CYBER BULLYING

6. **Understanding and discussion**. The Designated Safeguarding Lead (DSL), in conjunction with the Head of Computing, is responsible for overseeing the practices and procedures outlined in this policy and for monitoring its effectiveness. The DSL will report to the Head. In addition:

- Staff will receive training in identifying cyber bullying and understanding their responsibilities annually.
- All staff will be helped to keep up to date with the technologies that children are using.
- The pupils will be involved in developing and communicating a code of advice on protecting themselves from getting caught up in cyber bullying and on reporting cases they experience. They will have a voice through the School Council.
- Pupils will be educated about cyber bullying through a variety of means including assemblies, Anti-bullying Week, projects (ICT and PSHE), etc.
- Parents will be provided with information and advice on cyber bullying via literature, talks, etc.
- Students will be asked to sign the 'Rules for Student Network and use of the Internet' certificate (see ICT Policy) before they are allowed to use the internet in School.

- Pupils and staff will be involved in evaluating and improving policies and procedures.

7. **Policies and practices**. The School will:

   - Ensure that existing policies are reviewed and updated to include cyber bullying where appropriate.
   - Provide opportunities for pupils to contribute to this process.
   - Maintain records of all cyber bullying incidents and report regularly to the Governing Body.
   - Review the certificate regularly to ensure it remains appropriate as technologies develop.
   - Publish the rules and sanctions relating to this policy clearly and effectively.
   - Ensure there is effective online security measures in place (see Appendix 2).

8. **Promoting the positive use of technology**. The School will:

   - Make positive use of technology across the curriculum.
   - Use Continuing Professional Development opportunities to help staff develop their practice creatively and support pupils in safe and responsible use.
   - Explore ways of using technology to support assertiveness, self-esteem and to develop friendships.
   - Ensure all staff and children understand the importance of password security and the need to log out of accounts.

9. **Making reporting easier**. The School will:

   - Ensure staff can recognise non-verbal signs and indications of cyber bullying.
   - Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
   - Publicise to all members of the School community the ways in which cyber bullying can be reported.
   - Provide information for 'bystanders' including reassurances about protection from becoming victims themselves.
   - Provide information on external reporting routes e.g. mobile phone company, internet service provider, Childline.

RESPONDING TO CYBER BULLYING

10. Most cases of cyber bullying will be dealt with through the School's existing Anti-bullying Policy and Behaviour for Learning Policy. Some features of cyber bullying differ from other forms of bullying and may require a particular response. The key differences are:

- **Impact**: the scale and scope of cyber bullying can be greater than other forms of bullying.
- **Targets and perpetrators**: the people involved may have a different profile to traditional bullies and their targets.
- **Location**: the 24/7 and anywhere nature of cyber bullying.
- **Anonymity**: the person being bullied will not always know who is bullying them.
- **Motivation**: some pupils may not be aware that what they are doing is bullying.
- **Evidence**: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence.

It is possible that a member of staff may be a victim and these responses apply to them too.

11. **Support for the person being bullied**. The School will:

- Offer emotional support; reassure them that they have done the right thing in telling.
- Advise the person not to retaliate or reply. Instead, keep the evidence and take it to their parent or a member of staff.
- Advise the person to consider what information they have in the public domain.
- Unless the victim sees it as a punishment, they may be advised to change e.g. mobile phone number.
- If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively the School will contact the host provider and make a report to get the content taken down.
- If appropriate confiscate the mobile phone and ask pupil to delete the offending content and say whom they have sent it on to.
- Contact the police in cases of actual/suspected illegal content.
- If appropriate assist the person being bullied to block the person bullying from their sites and services.

12. **Investigation**. Instances of cyber bullying should be referred for investigation to the pupil's Head of Key Stage and recorded on MyConcern. If necessary the matter will be referred for further investigation to the Deputy Head and DSL. Staff and pupils should be advised to:

- Preserve evidence and a record of abuse; save phone messages, record or save-and-print instant messenger conversations, print or produce a screen-grab of social network pages, print , save and forward to staff whole email messages.
- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact: Internet Watch Foundation (www.iwf.org.uk), the local police or the Local Safeguarding Children Board Officer.

- Identify the bully impose appropriate sanctions and support in place for him / her.

Any allegations against staff should be handled as other allegations following guidance in Safeguarding Children and Safer Recruitment in Education.

13. **Working with the bully and applying sanctions**. The aim of the sanctions will be:

- To help the person harmed to feel safe again and be assured that the bullying will stop.
- To hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour.
- To demonstrate to the School community that cyber bullying is unacceptable and that the School has effective ways of dealing with it, so deterring others from behaving similarly.
- To apply sanctions for any breaches of policies or internet/mobile phone agreements.

In applying sanctions, consideration must be given to the type and impact of bullying and the possibility that it was intentional, in retaliation or unintentional. The outcome must include helping the bully to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the bully to change. Details on the type of sanctions are in the Behaviour for Learning Policy.

14. **Evaluating the effectiveness of prevention measures**. The School will:

- Use the School Council to hear the pupil's point of view.
- Identify areas for improvement and incorporate pupil's ideas.
- Conduct an annual evaluation including a review of recorded cyber bullying incidents, a survey of pupil and staff experiences and a parent satisfaction survey.
- Publicise evaluation findings; celebrate what works and what improvements are planned.

ADVICE TO PARENTS

15. Monitor the use of the internet at home by requesting to see recent sites used, ask to view the front page of your child's Facebook file, keep access to the internet downstairs in an open environment and avoid having a web cam in the bedroom. If your child looks unusually sad or withdrawn, gently enquire about their changed behaviour. Do contact the school or encourage your son or daughter to do the same; they may prefer to speak with a Peer Supporter/older pupil they trust or a trusted member of staff in the first instance; alternatively, an 'Independent Listener' or School Counsellor can be arranged via the School Nurse should your child ask to speak to a neutral advisor.

This policy was approved by the Academic Committee on 8 Oct 18

APPENDIX 1

FURTHER INFORMATION ON CYBER BULLYING

1. The Department for Education recommends various resources for dealing with cyber bullying including *The UK Safer Internet Centre* at www.saferinternet.org.uk and *CEOPS Thinkuknow* at www.thinkuknow.co.uk . There is also information on *The use of social media for on-line radicalisation* at https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation .

2. Cyber-bullying is an aggressive intentional act carried out by an individual or group using electronic media repeatedly over time against a victim who cannot defend him or herself. Seven categories of cyber-bullying have been identified:

- Text messaging: sending picture or video-clips.
- Phone calling
- E-mail messaging
- Defamatory blogs
- Personal websites
- Personal space
- On-line personal polling sites

These forms of bullying, regardless of whether or not they take place within school time, have a direct impact on the health and happiness of the intended victim. In the event that such bullying emanates from an individual or group within Battle Abbey School, the perpetrators will be subject to disciplinary action.

3. The advantages of technology are obvious to everyone and, used correctly, are a valuable resource. Sadly, there are those with less well adjusted attitudes who will seek to use these forms of communication to hurt people. The advice provided below is offered by Kidscape, a registered organisation whose purpose is to counteract all forms of bullying. You may wish to visit their website at www.kidscape.org for more information.

4. **Text/Video Messaging**. **Do not reply to abusive or obscene messaging.** Text (known as SMS or EMS) or video messaging (also known as MMS) should not contain anything offensive. **Report a problem**. Your mobile service provider will have a number that you can ring to report abusive messaging. Try their web sites for details. **Be careful of your personal details**. Do not give out your phone numbers without care and do not leave your mobile lying around when you are not about.

5. **Chat rooms or Instant Messaging (IM)**. **Do not give out personal information**. **Protect your identity**. Give yourself an alias that does not give out anything about your age, gender or location. **Think about what you write**. It is very easy for people to get the wrong idea about what you write or how you write it because they cannot hear the tone of voice it may be delivered in. **Never respond to abusive posting**. Ignore it or log off. If you do not take time off and calm down you might end up writing something you will regret. This would only escalate the matter.

6. **E-mail**. **Never reply** if you receive a nasty or abusive e-mail (known as being flamed). **Do not give them the satisfaction of a reaction**. If it is from someone you think you know, like someone at school, they want some kind of reaction, just like they would if they were standing in front of you and bullying you. Do not give them the satisfaction of replying. This may make them stop bothering you. **Find out where the e-mail is coming from if they do not stop**. Using an e-mail client like Outlook or Outlook Express, clicking the right mouse button over the e-mail will reveal lots of details about where and whom the e-mail came from. **Get your parents involved as early as you can**. They can contact the school or the service provider of the

sender of the e-mail. Make a hard copy or take a screen shot of the material if you can and retain it as evidence.

7. **Spamming**. The e-mail can also come from people that you do not know, as e-mail addresses are fairly easy for companies to obtain on the internet, using software called e-mail harvesters. They are also surprisingly easy for specialist programs to guess. **Under no circumstances reply to these types of e-mail**. Even if they have a 'Click here' and 'Stop receiving this e-mail' link - this will just confirm your e-mail address as a real one. The sender can then sell or pass it on to other people and you will be flooded with even more junk and abusive e-mails. You can delete the e-mails, but if the situation becomes serious, you should save them or print them off so that, if you need to take action, you have some evidence. **Learn more about your e-mail program from the 'Help' menu**. You should be able to find details of how you can create folders, e-mail filters and folder routing. This won't stop the e-mails, but it can help to shield you from them.

8. **Web**. If the cyber-bully is on a school or community website, do as you would do if the bullying was face to face - tell someone in that organisation.

APPENDIX 2

ONLINE SECURITY MEASURES

Battle Abbey School currently has the following Internet security measures in place and these are discussed at the half termly ICT meetings as necessary:

Fortinet Firewall and Web filters are installed at all sites including boarding houses. The web filters block websites / categories and applications.

Applications - Applications are signatures which contain a collection of ports that an App on a phone or a computer uses. For example, Snapchat is an application which uses a collection of ports, so the most efficient and secure way of blocking these types of things is by using application signatures. This is more advanced than general web filtering which can be bypassed.

Categories - Categories are for example "Terrorism" "Weapons" and many others. These are identified by the web filter and blocked.

Proxy protection – The web filter also provides proxy protection which prevents users from connecting to the internet via a proxy. This is a common method used by people who want to bypass web-filtering.

Virus and malware protection – The firewall scans all incoming internet traffic for viruses and malware which helps protect the school.

Intelligent filtering – The web filter is updated from an outside source to provide up to date application signatures which is crucial because commonly applications do change the ports that they use so without this in place the filtering would not be efficient.

Device management – All devices connecting to our network must be registered before they are able to access the internet. This allows us to track the devices and identify users who may be trying to do something that they should not be doing.

Reporting – All sites report their web activity to the main school reporting server. This generates traffic reports and also shows what sites / applications are allowed and what are blocked. This is a useful tool for tracking what a user has been doing and also to help identify a blocked application signature that needs to be unblocked.

Central Wireless Controller – Wireless can be switched off at given locations from the main management console on our firewall.