SPRATTON HALL

E-Safety & Cyberbulling Policy

September 2021

E-SAFETY & CYBERBULLYING POLICY

Title: E-Safety & Cyberbullying Policy	Responsible:	SJC / RPD / BJM / CJB / CMW
Date implemented: November 2009	Last Review:	September 2021
	Next Review:	September 2022

Introduction

This policy applies to all pupils at Spratton Hall including the EYFS (Reception children) who have access to and are users of the school's ICT systems. This policy must be read in conjunction with all of Spratton Hall's policies, paying particular attention to the School's Acceptable Use Agreements.

The 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.

The Designated Safeguarding Lead is responsible for E-Safety throughout the School and in this regard works closely with the Deputy Headmaster, Head of Computing, Head of PSCHE, Heads of Year and Form Tutors to ensure our pupils stay safe online and use ICT responsibly. The DSL is responsible for overseeing the practices and procedures outlined in this policy and for monitoring its effectiveness. She will report to the Head.

It is an important part of the School's pastoral care programme to ensure that pupils are provided with the education and resilience needed to protect themselves and their peers from online dangers. Technology is advancing rapidly and is now a large part of everyday life, education and business. However, it is important that all members of the school community are aware of the potential dangers of using the internet and understand the importance of using it appropriately. The School has a 'duty of care' towards any staff, pupils or members of the wider school community, to educate them in e-safety and this policy governs all individuals who are given access to the School's IT systems. This could include staff, governors, volunteers and pupils.

The School understands that some adults and young people will use technologies to harm children and there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in School, and providing members of the school community with a good understanding of appropriate IT use outside of school hours. E-safety does not just cover the Internet and available resources, but all different types of devices and platforms (e.g. mobile phone devices, wearable technology and other electronic communication technologies). These are accessible within the School for enhancing the curriculum, to challenge pupils, and to support creativity and independence.

Aims

The aims of this policy are to ensure that:

1. pupils, staff and parents are educated to understand what staying safe online and cyberbullying is and what its consequences can be
2. knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community
3. we have effective measures to deal effectively with cases of cyberbullying
4. we monitor the effectiveness of prevention measures
5. all pupils are confident, competent and independent users of ICT
6. pupils are provided with an understanding of how to use the internet and computer systems safely
7. pupils develop an appreciation of the use of ICT in the context of the wider world
8. the school provides ongoing training to pupils and parents; to ensure that they are educated and kept up to date with using the internet, including social media in a responsible and safe manner.

Background and Purpose:

- Pupils need to use digital and electronic resources as part of their education at Spratton Hall. These resources, owing to their nature may be subject to change and development.
- Pupils are required to be aware and adhere to the rules that form the Electronic Technologies Acceptable Use Agreements.
- The school is required to manage and use all data and information as described by the Data Protection Act 1998, the School's Data Protection Policy and Privacy Notice. The Bursar is the Data Controller for the School. Should a pupil have any questions relating to data then their Form Tutor or ICT teacher should be contacted in the first instance.

ICT and Computing Resources:

The school provides pupils with digital and electronic resources to use in order to enhance learning. These resources include:

- an internet supply, which is monitored and filtered for use by the school community
- a network account for pupils to create and store school work. All pupil work is created and saved on the Google Cloud
- a Google account which includes email and the use of Google Drive for pupils from Years 3-8. Our email service is Microsoft Outlook and Google is used for the Cloud
- Access to school computers several times a week, in both lesson and break-times
- Pupils in Years 6-8 are given a school Chromebook for use at home and at school
- Access to Edmodo, the 'virtual learning platform' the school uses for pupils in Years 4-8
- Access to the School's set of iPads or Chromebooks for class use
- Access to printers
- Access to a vast range of software and web-based resources

Appropriate Use of the School's ICT Systems

This guidance can be found in the *Electronic Technologies Acceptable Use Policy*.

- Pupils should understand that the school systems and devices are primarily intended for educational use and that they should not be used for personal or recreational use without permission.
- Pupils should understand that the school will monitor their use of the ICT systems, devices and digital communications for their own safety.
- A pupil should never attempt to access another person's email account.
- A pupil should never give their details to another person to use. If a pupil believes that someone else has accessed their email or Google account then they should speak to their Form Tutor, ICT Teacher or the ICT Technician
- Files should be saved to a pupil's folder in their Google Drive.
- Pupils are taught how to use the Internet safely and that they should not share personal information about themselves or others when online.
- Pupils are taught to be polite when communicating with others online. They should tell a teacher if they see something that upsets them on screen.
- It is expected that pupils should only print their school work when it is essential and avoid printing things unnecessarily.
- Pupils should take care of the School's ICT equipment, and report any breakages damage or faults, however it may have happened.
- Images and video should only be taken as part of the pupil's education with the knowledge and permission of a member of staff.
- Pupils should never install or attempt to install, or store any programmes of any type on school computer equipment. Nor should they attempt to alter any settings.
- Pupils should never attempt to by-pass the Internet Content Filter in order to access blocked websites.
- In accordance with the School's Electronic Technologies Acceptable Use Policy, pupils are not permitted to bring in mobile phones or other tablet devices to school. If a child has to bring a mobile or device into school, it should be handed in to their Form Tutor or the School Office and collected at the end of the school day. On rare occasions when pupils are permitted to use mobile phones, eg some residential trips, the school is aware that they may use 3G, 4G or 5G networks, and expects all pupils to act sensibly and safely. Inappropriate use may result in sanctions being imposed.

School Action:

- Staff will receive training in E-Safety and identifying cyberbullying and understanding their responsibilities. The DSL and Deputy Headmaster will liaise with the Head of Computing and Head of PSCHE on this matter.
- All staff will be helped to keep up to date with the technologies that children are using.
- The pupils will have a voice regarding developing codes of practice for E-Safety and preventing cyberbullying through the School Council, Tutor Group meetings and Digital Leaders.

- Pupils will be educated about E-Safety and cyberbullying through a variety of 'in-house' means: Computing and PSHCE lessons, form-time and assemblies
- Pupils across the whole school will be educated about E-Safety and cyberbullying from external sources including an annual visit from a specialist speaker, usually from ChildNet or Childline Online Safety
- Parents will be provided with information and advice on cyberbullying via literature and visiting speakers etc.
- Parents will be provided with information and advice on the legalities of contractual agreements with web companies and organisations.
- Pupils, staff and parents will be involved in evaluating and improving policies and procedures.
- Keep good records of all cyberbullying incidents

Cyberbullying

- Cyberbullying 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 can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyberstalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images; and manipulation

Making Reporting Easier

- Ensure staff can recognise non-verbal signs and indications of cyberbullying
- 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 cyberbullying 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 Cyberbullying

Most cases of cyberbullying will be dealt with through the school's existing Anti-Bullying Strategy and Behaviour and Sanctions Policy. Some features of cyberbullying differ from other forms of bullying and may prompt a particular response. The key differences are:

- impact: the scale and scope of cyberbullying 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 cyberbullying
- 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 usually have evidence of its occurrence
- it is possible that a member of staff may be a victim and these responses apply to them too
- specialist software is used for protection and recording

Support for the person being bullied

- 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, contact the host provider and make a report to get the content taken down.
- Contact the police in cases of actual/suspected illegal content
- In some cases, the person being bullied may be able to block the person bullying from their sites and services. Appendix 1 contains information on what service providers can do and how to contact them

Investigation

- 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 screenshot 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 the school's Designated Safeguarding Lead; the Local Authority or the local police.
- Identify the bully. See Appendix 2 for guidance
- Any allegations against staff should be handled as other allegations following school policy.

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 cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly

Sanctions

- In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation
- 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
- Spratton Hall will follow its own disciplinary procedures

Evaluating the effectiveness of prevention measures

- Use the School Council and Tutor time to hear the children's point of view
- Identify areas for improvement and incorporate children's ideas
- Conduct an annual evaluation seeking views from pupils, staff and parents

Legal duties and powers

- The school has a duty to protect all its members and provide a safe, healthy environment
- Head teachers have 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)
- School staff may request a pupil to reveal a message or other phone content and may confiscate a phone; they may not search the contents of the phone unless the school's discipline policy expressly states that right
- Some cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997

APPENDIX 1

When and how to contact the service provider

Mobile Phones

All UK mobile operators have nuisance call centres set up and/or procedures in place to deal with such instances. The responses may vary, but possibilities for the operator include changing the mobile number of the person being bullied so that the bully will not be able to continue to contact them without finding out their new number. It is not always possible for operators to bar particular numbers from contacting the phone of the person being bullied, although some phone handsets themselves do have this capability. Action can be taken against the bully's phone account (e.g. blocking their account), only with police involvement.
Details of how to contact the phone operators:

- O2: 08705214000 or ncb@O2.com
- Vodafone: call customer services on 191 from a Vodafone phone or on any other phone call 08700700191 for Pay Monthly customers or on 08700776655 for Pay As You Go customers.
- T-Mobile: call customer services on 150 from your T-Mobile phone or on 0845 412 5000 from a landline, or email using the 'how to contact us' section of the T-Mobile website at www.tmobile.co.uk.

Social Media (e.g. Facebook, Twitter, Snapchat, Instagram, YouTube)

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to 'Private,' so that only those authorised by the user are able to access and see their profile.

It is good practice for social network providers to make reporting incidents of cyberbullying easy, and thus have clear, accessible and prominent reporting features. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social networking sites do receive reports about cyberbullying, they will investigate and can remove content that is illegal or breaks their terms and conditions in other ways. They may issue conduct warnings and they can delete the accounts of those that have broken these rules. It is also good practice for social network providers to make clear to the users what the terms and conditions are for using the service, outlining what is inappropriate and unacceptable behaviour, as well as providing prominent safety information so that users know how to use the service safely and responsibly.

It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps

the most well-known of such sites, it is possible to report content to the site provider an inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself.

APPENDIX 2

Identifying the Bully

Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individuals' phone or hacking into their IM or school email account to send nasty messages.

In cases where you do not know the identity of the bully, some key questions to look at:

- Was the bullying carried out on the school system? If yes, are there logs in school to see who it was? Contact the school ICT staff or ICT support to see if this is possible.
- Are there identifiable witnesses that can be interviewed? There may be children who have visited the offending site and left comments, for example.
- If the bullying was not carried out on the school system, was it carried out on a mobile or a particular internet service (e.g. IM or social networking site)? As discussed, the service provider, when contacted, may be able to take some steps to stop the abuse by blocking the aggressor or removing content it considers defamatory or breaks their terms of service. However, the police will need to be involved to enable them to look into the data of another user.
- If the bullying was via mobile phone, has the bully withheld their number? If so, it is important to record the date and time of the message and contact the mobile operator. Steps can be taken to trace the call, but the mobile operator can only disclose this information to the police, so police would need to be involved. If the number is not withheld, it may be possible for the school to identify the caller. For example, another student may be able to identify the number or the school may already keep records of the mobile phone numbers of their pupils.
- Content shared through a local wireless connection on mobile phones does not pass through the service providers' network, and is much harder to trace. Similarly text messages sent from a website to a phone also provide difficulties for tracing for the internet service or mobile operator.
- Has a potential criminal offence been committed? If so, the police may have a duty to investigate. Police can issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message. This may help identify the bully. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact of behaviour).

A new national agency called the Child Exploitation and Online Protection Centre (CEOP) was set up in 2006 to deal with child sexual exploitation, and it is possible to report directly to them online at www.ceop.gov.uk However, it is important to note that it is the sexual exploitation of

children and young people, not cyberbullying, which forms the remit of CEOP. Information about cyberbullying and civil and criminal laws.

It is very important for schools to take cyberbullying seriously. It can be a very serious matter and can constitute a criminal offence.

Although bullying or cyberbullying is not a specific offence in UK law, there are criminal laws that can apply in terms of harassment, for example, or threatening behaviour, or indeed – particularly for cyberbullying – threatening and menacing communications.

APPENDIX 3

E-Safety During COVID-19 Measures

As the School has reopened after an extended period of distance learning, staff must be aware of the following potential online safety issues:

- We must recognise that children may have had more exposure to technology during lockdown.
- We must understand how this may have impacted children.
- Some children without access to technology may have been disadvantaged or isolated from their groups and peers.

As a school, we must therefore consider:

- that lockdown will have been a different experience for each and every child in the school;
- how we can support children following lockdown, including their mental health and well-being;
- how we can manage online learning in the future;
- how we can keep online safety a number one priority whilst discussing opportunities and risks around newly discovered online platforms and teaching tools;
- how we can best prepare for a second spike, including staff training.