SPRATTON HALL

# Online Safety & Cyberbullying Policy

September 2023

## Content

**ONLINE SAFETY & CYBERBULLYING POLICY**

| | |
|---|---|
| Title: Online-Safety & Cyberbullying Policy | Responsible: SJC / RPD / BJM / CJB / CMW |
| Date implemented: November 2009 | Last Review: September 2023 |
| | Next Review: September 2024 |

**Introduction**

This policy applies to all online community members 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. It sets out expectations with regards to online behaviour, attitudes and activities and use of digital technology.

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content.

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. It is essential that all stakeholders recognise that online/digital behaviour standards must be upheld beyond the school gates and school day, regardless of the device or platform.

Keeping Children in Education, 2023 Part 1 states; *"All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face".*

**Scope**

This policy applies to all members of the Spratton Hall community (including staff, governors, volunteers, pupils, parents/carers, visitors and community users) who have access to digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

**Definitions**

Where the following words or phrases are used in this policy:

References to **Designated Safeguarding Lead** (DSL) are references to the Designated Safeguarding Lead for the School.
References to **staff** includes all those who work for or on behalf of the School, regardless of their employment status, including supply staff, contractors, volunteers and Governors unless otherwise indicated.

**Aims**

The aims of this policy are to ensure that:

- Pupils, staff and parents at Spratton Hall are educated to understand what staying safe online and cyberbullying is
- Pupils adhere to the rules of the Electronic Acceptable Use Agreements
- All members of the school community are aware of the clear structures by which misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Behaviour and Sanctions Policy)
- Knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community
- Effective measures are in place to ensure a whole-school approach to educating the pupils about online safety; and that this is developed across all curriculum areas
- We have effective measures to deal with cases of cyberbullying
- We monitor the effectiveness of prevention measures
- All pupils are confident, competent and independent users of ICT
- Pupils are provided with an understanding of how to use the internet and computer systems safely
- Pupils develop an appreciation of the use of ICT in the context of the wider world
- The school provides ongoing training to staff, 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.

**Roles and Responsibilities**

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

**Headmaster – Mr Simon Clarke**
**Key responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the Designated Safeguarding Lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff

- Undertake training in online safeguarding
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the Data Protection Officer (DPO), DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

**Designated Safeguard Lead – Mrs Charlie Benn**
**(Supported by Deputy Designated Safeguard Leads – Miss Chloe Savage and Mrs Fiona Sanchez)**
The Designated Safeguarding Lead is responsible for Online 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.

**Key responsibilities** (the DSL can delegate certain online-safety duties, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2022):

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."

- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headmaster and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Alongside the Head of Computing, review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour and safeguarding)
- Receive regular updates in online safety issues and legislation, be aware of local and school trends

- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area
- Communicate regularly with the SMT Team, DPO and appropriate governors to discuss current issues and review any incidents (if necessary)
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware

**Governing Body Safeguard Link – Mrs Pam Long**
**Key Responsibilities**

- Approve this policy and strategy and subsequently review its effectiveness
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL / Head of Computing and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DSL, Headmaster and IT Manager to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure appropriate filters and appropriate monitoring systems are in place
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum

**Head of Computing – Mr Brendan McKenna**
**Key Responsibilities**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the Online Safety element of the Computing curriculum
- Ensure all member of the Computing team are aware of expectations for teaching Online Safety and provide appropriate resources
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with the IT Manager and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable use policy agreements
- Work with the Headmaster and DSL to ensure this document is reviewed and updated on a regularly basis

**Head of PSHCE – Mrs Cath Williams**
**Key Responsibilities**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCE Curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online

- Use the curriculum to complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCE

**Mental Health Lead – Miss Sally Fordy**
**Key Responsibilities**

- As listed in the 'all staff' section, plus:
- Develop a whole school approach to support mental health and to be aware of the role that the online world can play
- Work in conjunction with the Head of Computing and Head of PSHCE to ensure pupils are aware that online behaviour can sometimes lead to mental health issues
- Ensure staff and pupils are aware that establishing positive relationships and understanding empathy is equally important online as it is face-to-face
- Support staff and pupils in building digital resilience

**Network and IT Manager – Mr Vitor Fernandes-Neto**
**Key Responsibilities**

- Work with the Headmaster, DPO, DSL, Governors and Head of Computing to ensure frameworks are in place for the protection of data
- Ensure IT filtering systems are in place and monitored on a frequent basis
- Work with external senior technical engineer to maintain high levels of security
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Ensure that users may only access the networks and devices through a properly enforced password protected policy
- Ensure guests to the school are provided with a one-off school credentials to access the school wifi
- When appropriate, support staff in leading positive online safety initiatives in school

**Online Safety Team**
**Members:** Mrs Charlie Benn, Miss Chloe Savage, Mr Brendan McKenna, Mrs Cath Williams, Miss Sally Fordy and Mr Vitor Fernandez-Neto

**Key Responsibilities - in addition to roles outlined above;**

- Meet half termly and when necessary to review online safety provision within the school
- Act as point of contact on online safety issues and liaise with other members of staff as appropriate
- Ensure policies and procedures that incorporate online safety concerns are in place.
- Ensure there are robust reporting channels and signposting to internal, local and national support
- Ensure online safety is embedded throughout the curriculum and not isolated to Computing and PSHCE lessons
- Record online safety incidents and actions taken, in line with safeguarding policies

- Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse
- Liaise with the local authority and other local and national bodies as appropriate

**Specialist Computing Staff**
**Members:** Mr Brendan McKenna, Mr Oli Woodhouse, Mr Rob Wightman, Mr Toby Cowley
**Key Responsibilities**

- Deliver an effective Computing curriculum which includes a structured Online Safety Programme
- To ensure pupils are aware of the online world, the benefits and also elements to be wary of
- To utilise professional development opportunities to further enhance Computer Science knowledge
- To support all staff in areas related to computing and technology in school
- To regularly communicate with the Head of Computing for relevant updates to teaching provisions around Online Safety
- To promote good practise of technology throughout the school community

**All Staff**
**Key Responsibilities**
Staff understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.

- All staff know who the Designated Safeguarding Lead (DSL) is and who the Deputy DSLs are (Miss Chloe Savage and Mrs Fiona Sanchez)
- Read Part 1 of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, it is good practice for all staff to read all sections)
- Staff should read and follow this policy in conjunction with the school's main safeguarding policy
- Staff should be fully aware of the school's social media policy, which is included as part of the Staff Code of Conduct Policy
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Staff should be aware that the Child Protection/Safeguarding/Pastoral Care Concern Form can be found in the school's Safeguarding Policy
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- All staff have a responsibility to act as good role models in their use of technology
- Staff should also follow the Staff Acceptable Use Policy and Code of Conduct Policy.
- All staff are aware of the filtering systems that are in place to support them.

All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

- the sending of abusive, harassing and misogynistic messages;
- the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;
- the sharing of abusive images and pornography to those who do not wish to receive such content; and/or
- cyberbullying

Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:
(a) facilitates, threatens and/or encourages physical abuse;
(b) facilitates, threatens and/or encourages sexual violence; or
(c) is used as part of initiation/hazing type violence and rituals.

It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "just banter", "just having a laugh", "part of growing up" or "boys being boys" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. Staff should always be aware that these inappropriate behaviours can take place either online or offline, or in some cases take place simultaneously.

**Heads of Department / Subject Leads**
**Key Responsibilities**

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context (See Appendix 1)
- Work closely with the DSL, Head of Computing and Head of PSHCE to ensure an understanding of the issues, approaches and messaging that is been delivered around online safety
- Ensure subject plans also have an online safety element

**Volunteers**
**Key Responsibilities**

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

**Pupils**

**Key Responsibilities**

- Read, understand, and sign (electronically) the Electronic Technologies Acceptable Use Policy (Reception to Year 4) and (Year 5 to Year 8 including Chromebook Agreement)
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

**Parents / Carers**

**Key Responsibilities**

- Read, sign and promote the school's acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

The school is in regular contact with parents and carers and uses communications to reinforce the importance of ensuring that children are safe online. The school aims to help parents understand what systems are in place to filter and monitor their child's online use and ensures that parents are aware of what their children are doing online.

The school works closely with parents to ensure they can safeguard their children whilst using technology. Information is regularly sent through the newsletter and via talks for parents. Parents are also advised upon best practice and introduced to current trends during tutorial evenings. Please see Appendix 2 for a list of useful online safety resources for parents.

It is essential that the school educates parents on generational patterns and changes in online trends; a recent Ofcom report (March 2022) highlighted;

- Nearly all children went online in 2021 (99%); the majority used a mobile phone (72%) or tablet (69%) to do so
- Using video-sharing platforms (VSPs) such as YouTube or TikTok was the most popular online activity among children aged 3-17 (95%); while the majority chose to watch content on VSPs, 31% posted content they had made themselves, especially those aged 12-17

- Children still watch live television but are more likely to watch paid-for on-demand streaming services; 78% watched services like Netflix, Amazon Prime Video and Disney+, compared to 47% watching live TV. Scotland had the largest decline in broadcast viewing
- Six in ten children aged 3-17 played games online in 2021, increasing to three-quarters of 12- 17s

**Education and Curriculum**

While Computing and PSHCE are the two subjects that have the clearest online safety links (see relevant role descriptors above), it is the role of all Heads of Department and staff to identify opportunities, whether formally or ad hoc, to thread online safety through all school activities, both outside the classroom and within the curriculum. We recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt a wider cross-curricular overview. Technology is also included in the educational programmes followed in the EYFS.

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. Whenever overseeing the use of technology in school, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

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 all staff, pupils or members of the wider school community, to educate them in online safety and this policy governs all individuals who are given access to the School's IT systems.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright.

The school recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia, biphobia and sexual violence and sexual harassment.

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.

The school is also aware that while covid restrictions have lifted, the school community must remain vigilant on the needs of remote learning. See Appendix 3 for further guidance.

**Access to School Technology**

The School provides internet, intranet access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective Acceptable Use Policy when using School technology. All such use is filtered and monitored by the IT department.

The school IT resources also 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 5-8 are given a school Chromebook for use at home and at school
- Access to Google Classroom, the 'virtual learning platform' the school uses for pupils in Years 3-8
- Access to the School's set of iPads or Chromebooks for class use from Reception to Year 8
- Access to printers when required
- Access to a vast range of software and web-based resources
- Access to one or more desktop computers in each classroom in the Pre-Prep

**Inappropriate Material**

The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. KCSIE, 2022 highlights that "*the breadth of issues classified within online safety is considerable and ever evolving but it can be categorised into four areas of risk*";

(a) **Content** - being exposed to illegal, inappropriate or harmful content (e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism);
(b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);
(c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
(d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

**Filtering and Monitoring**

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their responsibilities. Spratton Hall School uses two tiers of filtering and monitoring. We receive filtering and monitoring through our network service provider NS Optimum and the school also uses the GoGuardian platform.

- **NS Optimum / Netsweeper** ensures that we have constant oversight of all devices connected to the school internet.
- Internet access is filtered for all users. Illegal content is filtered by the broadband / filtering provider by employing the Internet Watch Foundation list.
- **GoGuardian** provides filtering and monitoring for pupil Chromebooks. This system filters content and provides regular alerts to the IT team. This applies to Chromebook usage at school and remotely.
- All teaching staff have access to GoGuardian and this is used regularly in lessons to monitor pupils' online activity. Staff encourage appropriate use of the internet.
- Online provision for pupils is largely provided through our school Home Screen. This range of applications ensure safe access to educational resources while reducing the chance of inaccurate searching online.
- We endeavour to make sure our school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the school's filtering and monitoring provision. This is carried out by the IT Network Manager, the Online Safety Team and School Governors.
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password
- The Network and IT Manager is responsible for ensuring that software licence logs are accurate and up to date and those regular checks are made to reconcile the number of licences purchased against the number of software installations
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- Staff receive regular training related to Online Filtering and Monitoring.

**Infrastructure**

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- School infrastructure and individual devices are protected by up to date virus software

**Appropriate Use of the School's ICT Systems**

Pupils along with Parents/Guardians are expected to sign an electronic copy of the school's *Electronic Technologies Acceptable Use Policy*

In addition:

- 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 filter and 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, Computing 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 videos should only be taken as part of the pupil's education with the knowledge and permission of a member of staff. Please see our Data Protection Policy for more guidance on the use of photographs and videos.
- 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.
- 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.

## Handling Online Safety Concerns and Incidents

### School Action

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHCE). Staff will receive training in online safety and identifying cyberbullying and understanding their responsibilities.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

- All staff will be helped to keep up to date with the technologies that children are using.
- The pupils will have a voice regarding Online Safety and preventing cyberbullying through the School Council, Tutor Group meetings and Digital Leaders.
- The pupils can voice any safeguarding concerns through the schools Tootoot platform.
- Pupils will be educated about Online 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 Online 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.
- Pupils, staff and parents will be involved in evaluating and improving policies and procedures.

### Misuse by Pupils

Anyone who has any concern about the misuse of technology by pupils should report it immediately so that it can be dealt with in accordance with the School's Behaviour and Sanctions Policy, including the Anti-Bullying Policy where there is an allegation of 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

Please see **Appendix 4** for an overview of **cyberbullying**.

The table below highlights types of misuse and the policy which supports it;

| Type of Misuse | Relevant Policy | Reporting Avenue |
|---|---|---|
| Bullying | Anti-Bullying | Form Tutor / teacher or trusted member of staff. |
| Sexual harassment (whether during or outside of school) | Safeguarding Policy | The DSL, who has overall responsibility for online safety matters |
| Harassment | Safeguarding Policy | Form Tutor / teacher or trusted member of staff. Who should then refer to the DSL who has overall responsibility for safeguarding including online safety matters |
| Upskirting | Safeguarding Policy | |
| Radicalisation | Safeguarding Policy | |
| Other breach of acceptable use policy | See acceptable use policy | |

**Misuse by Staff**

Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

If anyone has a safeguarding related concern relating to staff misuse of technology, they should report it immediately in accordance with the school's safeguarding policy.

**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
- Reinforce pathways that allow pupils to report, such as the school's Tootoot platform
- Provide information for 'bystanders' including reassurances about protection from becoming victims themselves

**Responding to Online Bullying / Cyberbullying**

Most cases of cyberbullying will be dealt with through the schools 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:

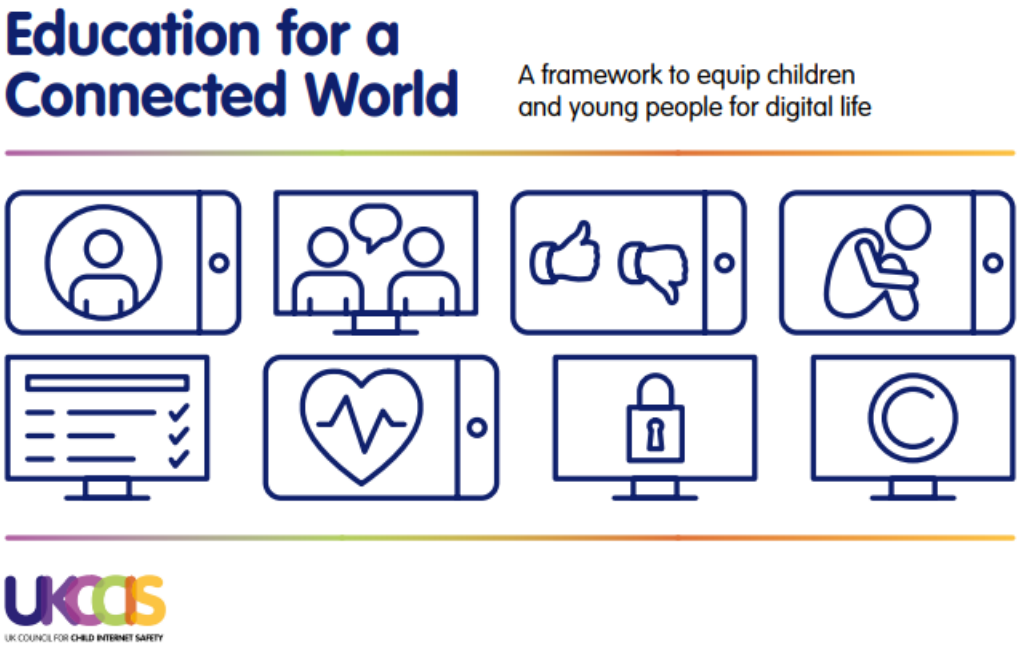
- Impact: the scale and scope of cyberbullying can be greater than other forms of bullying
- Targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets
- Location: the 24/7 and anywhere nature of cyberbullying
- Anonymity: the person being bullied 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

**Legislation**

Staff and stakeholders should be aware of the legislative framework under which guides the creation of any online safety policy. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. Please see Appendix 4 for a list of legislative frameworks.

**APPENDIX 1**

Education for a Connected World Framework




https://www.gov.uk/government/publications/education-for-a-connected-world

**APPENDIX 2**

**E-Safety During COVID-19 Measures**

As the School has fully reopened after periods of distance learning over the last few years, staff must be aware of the following potential online safety issues:

- We must recognise that pupils may have had more exposure to technology during lockdown periods.
- We must understand how this may have impacted pupils.
-
- As a school, we must therefore consider:
- that lockdown will have been a different experience for each and every pupil in the school;
- how we can support pupils following lockdown periods, including their mental health and well-being;
- how we can manage online learning in the future; and,
- how we can best prepare for future events of remote learning

**APPENDIX 3**

Useful online safety resources for parents

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers
(b) http://www.childnet.com/parents-and-carers
(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/onlinesafety/
(d) https://www.thinkuknow.co.uk/parents/
(e) https://www.thinkuknow.co.uk/parents/articles/theres-a-viral-scare-onlinewhat-should-i-do/
(f) http://parentzone.org.uk/
(g) https://www.internetmatters.org/
(h) https://www.commonsensemedia.org/
(i) Advice for parents and carers on cyberbullying (DfE, November 2014)
(j) https://www.askaboutgames.com/
(k) https://www.ceop.police.uk/safety-centre

**APPENDIX 4 - CYBERBULLYING**

Cyberbullying is bullying that takes place using technology. It can take the form of many behaviours including:

- Harmful messages (text, instant, multimedia, email)
- impersonating another person online
- sharing private messages
- uploading photographs or videos of another person that leads to shame and embarrassment
- creating hate websites/social media pages
- excluding people from online groups

Pupils should remember the following:

- use the security settings when using technology.
- regularly change your password and keep it private.
- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- If you or someone you know are being cyberbullied, tell someone. You have the right not to be harassed or bullied online. Tell an adult you trust - your parents, any member of staff or volunteer, or a helpline such as ChildLine on 0800 1111.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the School to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.
-

You may find the following websites helpful:

https://www.childnet.com/young-people/
https://www.childnet.com/resources/smartie-the-penguin/
https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/
https://www.bbc.com/ownit
https://www.thinkuknow.co.uk/
https://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx
https://www.saferinternet.org.uk/advice-centre/young-people
https://mysafetynet.org.uk/

Please see the School's Acceptable Use Policy for Pupils which sets out the School rules about the use of technology including mobile electronic devices.

**APPENDIX 5**

**Computer Misuse Act 1990**
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

**Data Protection Act 1998**
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

**Freedom of Information Act 2000**
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

**Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (eg YouTube).