Grimsargh St Michael's C of E Primary School

Online Safety Policy

January 2022

Let your light shine before people so that they may see your good works and glorify your Father in heaven (Matthew 5: v.16)

Inspiring, believing and achieving in our loving Christian community

Statement of intent

At Grimsargh St Michael's C of E Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst we recognise the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

We have created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff as well as all other visitors, including governors, students and volunteers. We are committed to ensuring children have the necessary tools needed to embrace technology throughout their lives whilst providing a safe teaching and learning environment. We have implemented important controls to mitigate the risk of harm.

KCSiE (2021)

This policy will, in line with the 2021 KCSiE statutory guidance, outline the procedures in place to control the four areas of risk associated with Online Safety:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Context

Pupils at Grimsargh St Michael's Primary School have access to a range of online materials that enrich and extend teaching and learning opportunities. The benefits to teaching and learning are many and varied.

Pupils will be given clear objectives for Internet use and will access material under guidance from their class teacher. Teachers will supervise pupils and take all reasonable precautions to ensure that users only access material appropriate to their learning. Pupils are taught to use technology safely and respectfully, keeping personal information private and are taught to identify where to go for help and support, and when they have concerns about content or contact on the internet or other online technologies.

Remote Learning

We are committed to supporting our pupils in accessing learning content online from home and see online material as a key element of our approach to blended learning in light of the Coronavirus Pandemic. Please see our Remote Learning Policy. Staff use our school website alongside the online platform 'SeeSaw' to communicate with children and their parents/ carers.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance and Keeping Children Safe in Education 2021 (KCSiE). It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the General Data Protection Regulation (2018) and the Equality Act 2010. The policy also reflects the National Curriculum Computing Programmes of Study.

This online safety policy will be used in conjunction with the following school policies and procedures:

- Safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Use of mobile phones statement

Roles and responsibilities

Governors

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. It is the responsibility of the Governor responsible for Online

Safeguarding to ensure that this document is tabled at least annually at the termly meeting of the full Governing Body or at the first meeting following any major incident. The Online Safety link governor will organise a termly meeting with the headteacher and/ or computing leader to discuss online safety.

The link governor for online safety is Mr Jonny Galbraith.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The DSL is Mr Stuart Booth (headteacher) and deputy DSL is Miss Helen Smith (deputy headteacher). The DSL and deputy have responsibility for online safety in school, in particular to:

- Ensure this policy is being implemented consistently throughout the school.
- Ensure that all staff are aware of the reporting procedures and requirements should an online safety incident occur.
- Work with staff, as necessary, to address any online safety issues or incidents.
- Ensure that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged (CPOMS) and dealt with appropriately in line with the school behaviour policy.
- Update, deliver and/ or organise staff and parent training on online safety.
- Liaise with other agencies and/or external services if necessary.
- Work alongside the online safety link governor to provide regular reports on online safety in school to the governing board.

Computing/ Online Safety Leader and Technician

The computing/ online safety leader and technician are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the headteacher receives the weekly monitoring report.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.

- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL and deputy to ensure that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged (CPOMS) and dealt with appropriately in line with the school behaviour policy.
- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils

Pupils are expected to:

- Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials.
- To 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 behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.
- To contribute to any 'pupil voice'/ surveys that gathers information of their online experiences.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- Monitor their child's usage of communications technologies and report any concerns to the headteacher.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support;
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents;
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying;
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls;
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world;

- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation;
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online;
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online);
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online;
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games;
- Parentzone provides help for parents and carers on how to keep their children safe online;
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations;
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online.

Visitors

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. They will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Our Grimsargh St Michael's Primary School Computing Curriculum outlines the content of online safety teaching and learning.

Educating parents about online safety

We believe in working closely with our parents to support pupils in developing safe practice when using online technology and therefore provide updates through our newsletter and website. Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any Online Safety related concerns. Training is also offered to our parents each academic year.

This policy is shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL or deputy.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See also our school Anti-Bullying and Behaviour policies.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure, mainly through the Computing Curriculum, that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the wider curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding. The school also signposts parents to information on cyber-bullying so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Security and Data Management

In line with the requirements of the General Data Protection Regulation (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.
- All laptops/chromebooks are password protected.

All children have class or individual passwords and are encouraged not to share. All data in the school is kept secure and staff are informed of what they can or can't do with data through the Online safety Policy and statements in the Acceptable Use Agreements.

- The school maps key information that is held.
- There is a named person, Mr Stuart Booth (headteacher) with responsibility for managing information.
- Relevant staff know the location of data.
- All staff with access to personal data understand their legal responsibilities.
- The school ensures that data is appropriately managed, both within and outside the school environment, through the use of secure emails.
- All staff are DBS checked and records are held in a single central record
- Staff are aware that they should only use approved means to access, store and dispose of confidential data.
- Pupil data is kept for 25 years and safely disposed of by the school's Data Protection Officer.
- Personal devices, e.g. Smartphone, iPads may not be used to access data on the school system.
- Risk of data loss is minimised by having daily back up of the administration networks and weekly back up for the curriculum network.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer.
- All servers are managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

Mobile phones/ Electronic devices

Pupils at Grimsargh St Michael's Primary School are not permitted to bring mobile phones or other devices into school unless there are exceptional circumstances which have been agreed by the headteacher. In these circumstances, mobile phones must be handed into the school office. If a phone is brought in by mistake or for the child's journey to and from school then pupils are asked to hand in the phone to the school office for safe keeping until the end of the day.
If inappropriate material is found on a pupil's electronic device, the DSL and/ or deputy DSL along with the online safety leader will decide whether they should:

- Delete the material
- Retain it as evidence (of a criminal offence or a breach of school discipline)
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Mobile phones may be used by staff and visitors at appropriate times and only to be used in the staffroom during school hours. Staff and visitors are allowed to use mobile phones in classrooms, out of hours, when pupils are not present. It is expected that staff and visitors turn their mobile phones on silent during curriculum time. However, in exceptional circumstances prior arrangements can be made with the Headteacher.

Staff must store mobile phones in their lockers unless needed on their person for an exceptional circumstance. Phones may be checked for missed calls and messages at break and lunchtimes. **Mobile phones are not permitted in the playground or in rooms where children are present.**

A personal mobile phone can be used for school educational visits/ and sports or other school events as often multiple members of staff are in attendance and one school phone would not be adequate. Staff must only use their phone to contact other staff members on the visit, as needed, or for emergencies.

Network

To ensure the network is used safely, we:

- Ensure staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.

- Provide all pupils from year 2 upwards with their own unique username and password which gives them access to the Internet and other services.
- Make clear that no one should log on as another user and that pupils should never be allowed to log-on or use teacher and staff logins.
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Require all users to log off when they have finished working or are leaving the computer unattended.
- Ensure all equipment owned by the school and/or connected to the network has up to date virus protection.
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used primarily to support their professional responsibilities.
- Make clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintain equipment to ensure Health and Safety is followed.
- Ensure that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems.
- Do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
- Have a clear disaster recovery system in place that includes a secure, remote off site back up of data.
- Use secure data transfer- this includes DfE secure S2S website for all CTF files sent to other schools.
- Ensure that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Use a wireless network that has been secured to appropriate standards suitable for educational use.
- Have IT and communications systems that have been installed professionally and are regularly reviewed to ensure they meet health and safety standards;

Password policy

- It is made clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff using critical systems (e.g. CPOMS, Pupil Tracker) to use two factor authentication.

E-mail

At Grimsargh St Michael's, we:

- Provide staff with an email account for their professional use, LA email and makes clear personal email should be through a separate account;
- Use anonymous or group e-mail addresses, for example info@grimsargh-st-michaels.lancs.sch.uk/ head@grimsargh-st-michaels.lancs.sch.uk/ or class e-mail addresses.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date
- Use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Staff

- Staff can only use the LA e-mail systems on the school system.
- Staff will use LA e-mail systems for professional purposes.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption. SLT and Office only to have secure e-mail access to certain data.

School website

A school website and other online publications provide an effective way to communicate information. The following statements are what our school deems acceptable and unacceptable use of web sites and other online publications:

- The Headteacher, supported by the Governing body, and in particular the governor with responsibility for website compliance, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school web site complies with statutory DFE requirements.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- Staff or pupil personal contact information will not be published. The contact details given online will be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The nominated governor is responsible for ensuring that content is accurate and appropriate.
- Pupils full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published.
- The school website will be used to communicate Online safety messages to parents/carers, to provide guidance on the use of digital media.
- Downloadable materials will be in read-only format (e.g. PDF) to prevent content being manipulated and potentially re-distributed without the school's consent.

Social Networks:

In our school, the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- There should be no accessing of personal social networks on school equipment.
- Staff are strongly advised to avoid putting personal information/photos on social networking sites which parents and children can access.
- Staff are discouraged from being 'friends' with parents/ carers of children attending school.

Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display.

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form annually or when their child joins the school. However, parents have a right to change this during the academic year if deemed necessary.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other publications the school will obtain individual parental permission for its use.
- The school will not re-use any photographs or videos after staff and pupils have left the school without further consent being sought.
- Parents/carers, who have been invited to attend school events, are not allowed to take videos and photographs of their child with other children unless given permission by the headteacher/ deputy headteacher.
- All staff recognise and understands the risks associated with publishing images, particularly in relation to use of personal Social Network sites. It is forbidden for staff to post images or video of pupils taken at school, in any school activities, on any Social Network sites, other than those of the school.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are not allowed to store digital content on personal equipment. Staff are not to use their own cameras. If used, this will be recorded as a low-level concern.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the headteacher, SLT and Governors on an annual basis.

Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Dealing with incidents

All incidents must be reported to the Headteacher. Records are audited on a regular basis by the Headteacher and Computing/ Online Safety leader.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Potential illegal content must always be reported to the Internet Watch Foundation (http://www.iwf.org.uk)

Examples of illegal offences are:

1. Accessing child sexual abuse images
2. Accessing non-photographic child sexual abuse images
3. Accessing criminally obscene adult content
4. Incitement to racial hatred

More details regarding these categories can be found on the IWF website; http://www.iwf.org.uk

Inappropriate use

It is more likely that at school we will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	Procedure and Sanctions
Accidental access to inappropriate materials	• Minimise the webpage /turn the monitor off/ turn the iPad off. • Tell a trusted adult. • Staff enter the details into the incident log and report to LGFL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously	• Inform Online Safety leader/ Headteacher • Enter the details in the Incident Log • Additional awareness raising of Online Safety issues and the Acceptable Use Policy with individual child/class • More serious or persistent offences may result in further disciplinary action • Parents/Carers informed
Deliberate searching for inappropriate materials	
Bringing inappropriate electronic files from home	
Using chats and forums in an inappropriate way	

Online safety incidents will be reported to the Online Safety leader who will record the incidents in CPOMS. The Online Safety leader will report all incidents to the Headteacher to discuss appropriate actions to be taken.

- All staff are aware of the different types of online safety incidents and how to respond appropriately.
- All pupils are informed of procedures through discussions from members of staff.
- Incidents are monitored by the online safety leader and Headteacher on a regular basis
- The Headteacher will decide on which point that parents or carers are informed.
- The procedures are in place to protect staff and escalate a suspected incident/ allegation involving a staff member.

Continuing Professional Development

All staff members will receive Safeguarding training, including new members of staff as part of their induction, which will include online safety, including cyber-bullying, and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Safeguarding Policy.

Monitoring and Filtering

Filtering and virus protection at Grimsargh St Michael's are carried out via Netsweeper and Sophos AV. We have control of assignments and filtering policies, excluding categories that are deemed inappropriate by default.

Online activity of staff, children and visitors to school is monitored and a report is generated on a weekly basis. This is monitored by the headteacher and computing/ online safety leader and outcomes shared as necessary with the school leadership team. Any concerns that arise are reported immediately to our Designated Safeguarding Leader (Mr S Booth), Deputy DSL (Miss Helen Smith) and/ or Online Safety Lead (Miss E Threlfall). Action is taken immediately to address any concerns that arise- in line with our Behaviour, Anti-Bullying, Safeguarding policies and procedures- this is reported to the Governing Body.

This policy will be reviewed by the Headteacher and computing/ online safety leader. At every review, the policy will be shared with the full governing board.

Signed**: Mr Stuart Booth**

Date: **January 2022**

Review Date: **September 2022**

Agreed by the Curriculum Committee**: 7th February 2022**