Hippings Methodist Primary School
Heron Way
Oswaldtwistle

Written By: **Sept 2024**	**D.Eccles**
Date:	**Sept 2025**
Checked by:	**Mrs T Westwell (headteacher and DSL)** **Mrs M Hunter(Deputy Head and DSL)** **Chair of Governors: Mrs M Gardner**
Review Date:	**Sept 2026**

Contents:

1) **Purpose**
2) **Aims**
3) **Roles and responsibilities:**
    - **Teachers and Staff**
    - **Governors and Senior Leadership Team**
    - **Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL)**
    - **Children and Young People**
    - **Teachers and Support Staff**
    - **Technical Staff**
    - **Parents and Carers**
4) **Filtering and Monitoring**
5) **Education**
6) **Curriculum**
7) **Reporting**
8) **Use of digital images**
9) **Acceptable Use**
10) **AI**

1) Purpose:

The purpose of this policy is to safeguard and protect all members of Hippings Methodist Primary School online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of Hippings Methodist Primary School This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of Hippings Methodist Primary School digital technology systems, both internally and externally.

2) Aims of this policy:

This policy supplements the Safeguarding Policy in setting out clear guidance and procedures. The policy provides information and clear guidance for all stakeholders and staff within school. At Hippings Methodist Primary School, we aim to help every pupil and adult to:

• Feel safe and confident when using new technologies.

• Know who to speak to when they feel unsafe.

• Know how to report any abusive behaviour.

• Know how to use the internet correctly, without misuse.

• Know what device is appropriate to use and when/where to use it.

• Identify a potential risk or situation from the onset.

• Stay in control and keep personal information private.

• How to take the necessary measures to block and delete accounts, messages and people.

3_Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within *[Hippings Methodist Primary School].*

Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; head teacher, teachers, substitute teachers, work-experience staff, office staff, nurses, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.

Governors and Senior Leadership Team

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the senior leadership team, the online safety lead and computing lead.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.

- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

Children and Young People

With respect to online safety in your school, children need to:

- Know who the DSL is.
- Engage in age-appropriate online safety education opportunities.
- Contribute to policy development and review.
- Read and adhere to online safety policies.
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Where and how to find help with any online incidents or concerns.
- How, when and where to report concerns and when to seek help from a trusted adult.

Teaching and Support Staff:

Teaching and Support Staff are responsible for:

- ensuring they stay up to date with current Online Safety matters and policies and practice.
- reading, understanding and complying with the school's Acceptable Use Policy (AUP).
- reporting any misuse by children or staff to the Online Safety Co-ordinator/Head Teacher for further investigation via the CPOMs software.
- emailing any technical problems to the school's Bursar who will in turn log these with the ICT technical support staff.
- ensuring that any digital communications with pupils, for example email and learning platforms, should be strictly professional and only carried out using school systems.
- following the current computing scheme Kapow adopted by the school to ensure that the teaching of Online Safety is embedded throughout the computing curriculum.
- that pupils understand and follow the AUP and Online Safety policy.
- being aware of Online Safety issues relating to the use of mobile phones, cameras, smart watches, websites, games and handheld devices/wearable technology and that they monitor their use and implement current school policies with regard to these devices.
- Being aware of the use of AI

Technical Staff:

- The ICT technical support staff are responsible for ensuring that:
- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- the school meets the Online Safety technical requirements outlined in the Lancashire Online Safety Policy Guidance.
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.

- he/she keeps up to date with relevant Online Safety technical information and guidance in order to carry out their role effectively.
- monitoring software/ systems are implemented and updated regularly.

** Currently, the school has a package with BT Lancashire Education Digital Services **

Parents/Carers:

Parents and carers have the responsibility to ensure that their children use their internet enabled devices appropriately and do not misuse these technologies. Parents are made aware of the school's AUP and Online Safety Policy through the school website. The educating and/or providing further information around the AUP and Online Safety Policy is provided through newsletters, assemblies and links online via the school's website. Parents and Carers also have access to the National Online Safety website.

4) Filtering and Monitoring:

Hippings Methodist School receives a filtered broadband service. This service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal.

The service is managed by BT Lancashire Education Digital Service and the school's SLT with oversight from the Governor responsible for IT. This allows for the service to be flexible, so the school can have ownership of what else needs to be filtered as technology advances.

The broadband is supplied by Lancashire County Council Education Digital Services: further information can be found at

https://educationdigitalservices.lancashire.gov.uk/security-online-safety.aspx

Netsweeper is our school's filtering solution. It is a hardware-based content filtering solution built to provide schools with an even more comprehensive content filtering solution

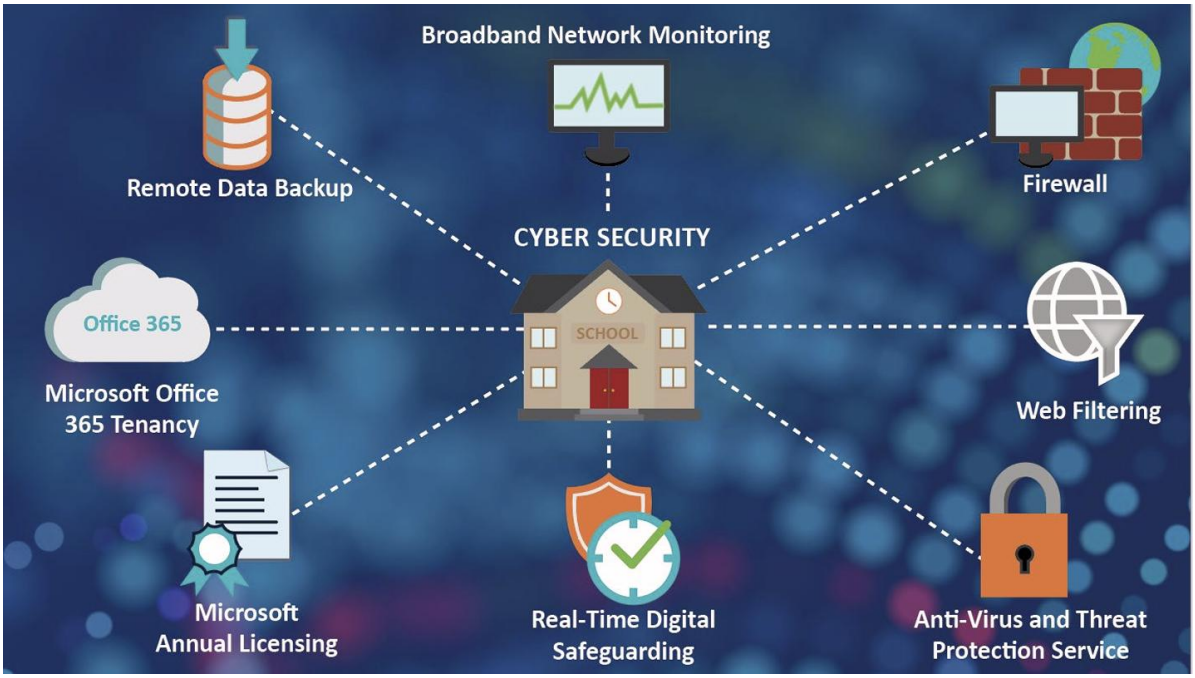
Along with all the basic features of *****, ***** offers an even greater level of control over the school's filtering. The school is able to filter the content of both HTTPS and HTTP sites in the same way, while establishing different filtering profiles for any group of users, computers, or user accounts. It also gives the school a tool for monitoring the content

that is being requested on the internet.

The monitoring of pupil and staff devices is done via the Netsweeper Software. The software is set up with both default and bespoke alerts which notify a member of the Senior Leadership Team if a breach occurs.

Please click on the link for more information:

cyber-security-diagram.pdf



5) Education:

All children will receive planned Online Safety lessons throughout Computing and PSHE lessons. These lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of lessons, worships and weekly newsletters to ensure all children are aware of the matter. They will also be taught to question the validity of the information they find online. Parents receive information via parent's evenings, weekly Online Safety posts, newsletters and links via the school's website.

It is each staff member's wider professional responsibility under the safeguarding of children to read and understand the Online Safety Policy. All staff are required to read and understand the elements of Online Safety stated within the latest version of Keeping Children Safe in Education (KCSIE) as part of their wider Safeguarding responsibility. All new staff are directed to read the Online Safety Policy Document as part of the induction process to ensure they are fully aware and understand the Online Safety. Once in receipt of the policy document, either in a physical form or directed to its online form, it is presumed they understand the policy, unless they seek further advice. The Online Safety Co-ordinator will be able to respond to regular updates provided by Lancashire LEA or other training schemes and report back to staff any new issues that they need to be aware of by either email or an arranged meeting. The Online Safety Co-ordinator will provide guidance for any member of staff that seeks it.

6) Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the pupils visit and

should remind the children what to do in the event of seeing an inappropriate image prior to starting the lesson. It is accepted that from time to time, for good educational reasons, students may need to research topics during lessons (e.g. weapons - which could be part of a study on the Roman Army) that would normally result in internet searches being blocked. In such a situation, staff should obtain permission from a member of the school's SLT and then request a Page 5 temporary removal of those sites from the filtered list for the period of study contacting BT Lancashire Educational Digital Services. Any request to do so, should have clear reasons to support the need of these websites.

7) Reporting :

All staff must report any safeguarding concerns regarding online safety through the school's reporting system, CPOMS and a DSL notified as soon as possible.
Further detail on the school's Safeguarding Report Procedure can be found within the school's Safeguarding Policy.

8) Use of Digital Video and Digital Images:

The developments of digital images and videos have significant benefits within the curriculum and can enhance learning.
Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.
When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet and on social networking sites.
Members of staff are allowed to take digital/video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images, as well as personal information. Further details can be found in the school's policies and procedures related to the General Data Protection Regulation (GDPR).
The school has a clearly displayed list which states where parental permission has been declined for specific pupils to not have their photos taken and/or published online. Any photographic image should only be taken on school equipment unless prior permission is gained from the headteacher e.g. residential trips whereby the photos must be deleted as soon as possible.
Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.
Permission must be obtained from the parent or carer of any child before pictures are published on the website. Written permission is provided for every child that starts school to indicate whether the parent or carer allows their child to be photographed.

9) Acceptable Use:

All users of the computers will be made aware of what is acceptable or not by the AUP. If unacceptable use is conducted, the correct procedures and sanctions are in place.
It is expected that all users will be responsible and safe users of ICT, who understand the policy and work within it.
However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

Examples of illegal activity:
• child sexual abuse images
• extremist material
• adult material which potentially breaches the Obscene Publications Act
• criminally racist material
• other criminal conduct, activity or materials
If any apparent or actual misuse appears to involve illegal activity, like those examples listed above, the correct reporting procedure is in place and all staff are aware to inform the Head Teacher, Child Protection Officer and/or the SLT immediately, who will then investigate the matter. All children will be made aware of the importance to report any incident to either an adult at school that they can trust.
If an incident has occurred due to carelessness, which will be more likely the case, this will to be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements of the policy.

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:
• ensuring that personal information is not published.
• education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
• clear reporting guidance, including responsibilities, procedures, and sanctions.
• risk assessment, including legal risk.
• guidance for learners, parents/carers

School staff should ensure that:
• No reference should be made in social media to learners, parents/carers or school staff.
• they do not engage in online discussion on personal matters relating to members of the school community.
• personal opinions should not be attributed to the school.
• security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
• they act as positive role models in their use of social media
When official school social media accounts are established, there should be:
• a process for approval by senior leaders
• clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
• a code of behaviour for users of the accounts

• systems for reporting and dealing with abuse and misuse
• understanding of how incidents may be dealt with under school disciplinary procedures.

10) Artificial Intelligence (AI):

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Our school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully pupils very seriously, in line with our school's behaviour policy.