St Mary's Hampton
Church of England Primary School

ONLINE & E-SAFETY POLICY

Including Acceptable Use Agreements for Pupils, Parents/Carers, Staff, Governors, Visitors & Volunteers

Agreed by LGC:	Spring 2025
Review Frequency:	Annual
Next Review:	Spring 2027

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteacher and school staff
- Relationships and sex education
- Searching, screening and confiscation

This policy also:

- refers to the DfE's guidance on protecting children from radicalisation.
- reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it

reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

- Accounts for the National Curriculum computing programmes of study.
- complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The local governing committee

The local governing committee has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The local governing committee will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The local governing committee will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The local governing committee will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding leads (DSLs).

The local governing committee should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The local governing committee must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The safeguarding link governor will review the DfE filtering and monitoring standards, and will ensure the school's IT service provider supports the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational

needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The designated safeguarding leads

Details of the school's designated safeguarding leads (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Senior Leadership Team and local governing committee to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Senior Leadership Team, IT service provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's safeguarding and child protection policy
- Ensuring that any online safety incidents are logged on the school's safeguarding management system (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
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or local governing committee
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT service provider

The ICT service provider, Eduthing, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring 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 any online safety incidents are logged using the school's online safeguarding management tool (CPOMS) and dealt with appropriately in line with this policy
- Ensuring any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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 (appendix 3), and ensuring pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by recording it using the school's online safeguarding management tool (CPOMS)
- Following the correct procedures by informing the IT Service Provider, Eduthing, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure any online safety incidents are logged on the school's online safeguarding management tool (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or 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 (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All primary schools have to teach Relationships education and health education.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- People sometimes behave differently online, including by pretending to be someone they are not
- The same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications sent home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- The systems the school uses to filter and monitor online use
- The activities their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers 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.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Use of Knowsley Council Online Safety Materials

At St Marys Hampton, we actively use Knowsley Council's online safety and e-safety materials to support a consistent, high-quality approach to educating pupils, staff and families about staying safe online. These resources underpin our whole-school approach and ensure our practice reflects local authority guidance and current risks.

Knowsley Council materials are used to:

- Inform the design and sequencing of our computing and PSHE curriculum, ensuring online safety is taught in an age-appropriate and progressive way from Early Years through to Year 6.
- Support staff in delivering clear, accurate and confident online safety messages, including guidance on emerging risks such as social media, gaming, livestreaming and artificial intelligence.
- Provide assemblies, lesson resources and discussion prompts that help pupils understand how to keep themselves safe, recognise unsafe situations, and know how and where to seek help.
- Strengthen staff awareness through safeguarding and online safety training, enabling adults to identify concerns, respond appropriately to incidents, and model safe online behaviour.
- Engage parents and carers through shared guidance, links and information from Knowsley Council, helping families reinforce safe online habits at home.

These materials are reviewed regularly by the Designated Safeguarding Lead and computing lead to ensure they remain current and responsive to local and national priorities. By embedding Knowsley Council's guidance into our curriculum, training and communication with families, St Mary's ensures that online safety is a shared responsibility and an integral part of our safeguarding culture.

6. Cyber-bullying

6.1 Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- No**t** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 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 Bard.

St Mary's Hampton recognises 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.

St Mary's Hampton will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

As per the mobile phone policy, pupils may bring mobile devices into school if they are travelling to and/or from school by themselves but are not permitted to use them during the school day. Phones must be handed in to the class teacher, to be locked in a drawer until dismissal.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT service provider, Eduthing.

10. 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 our policies on behaviour and ICT and internet acceptable use. 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 procedure / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents involving illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSLs and DDSLs 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 child protection and safeguarding policy.

12. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the local governing committee. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedure
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use statements (appendices 1 to 3).

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ICT User Agreement

All the employees of St Mary's Hampton CE Primary School (the School) have the opportunity to use the school's extensive ICT resources. To qualify to use these resources all staff need to read and agree to the terms of this ICT user agreement.

The school strongly supports the use of ICT and every effort will be made to provide reliable resources to all users, however inappropriate and/or illegal use of any ICT resource is strictly prohibited.

Please take some time to read the following document carefully. Listed are the provisions of the agreement, if any user violates this agreement access to ICT resources will be denied and the user may be subject to disciplinary action.

Acceptable Use: All Users

1. Personal Responsibility

As a representative of the School, you will accept personal responsibility for reporting misuse of ICT resources to a member of the Senior Leadership Team. Misuse may come in many forms, but is commonly viewed as any information sent, received or viewed that indicates or suggests pornography, unethical or illegal activities, racism, sexism, inappropriate language or any use of which may be likely to cause offence.

2. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include but are not limited to the following:

- BE POLITE. Never send or encourage others to send, messages with abusive material.
- USE APPROPRIATE LANGUAGE. Remember that you are a representative of The School. Never use inappropriate language. Discussion of Illegal activities is strictly prohibited.
- PRIVACY. Do not reveal any personal information to anyone especially the home address or personal details of yourself or any others.
- E-MAIL. Electronic Mail (E-Mail) is not guaranteed to be private. Messages are screened for inappropriate material, and although in most cases this takes place automatically, your message may be individually screened. Messages supporting illegal or inappropriate activities may be reported to the relevant authorities.
- DISRUPTIONS. Do not use the ICT resources in a way that could be disruptive to others.
- OTHER CONSIDERATIONS. Remember that humour and satire are very easily misinterpreted. Respect the rights and beliefs of others.

3. Services

The school makes no guarantees of any kind whether expressed or implied for the ICT service that is provided. The school denies any responsibility for the validity or accuracy of any information obtained by its internet services. We do not recommend or endorse the storage of data outside of our network. If information is stored locally, for example on a laptop, the individual user is responsible for ensuring that their data is securely backed up.

4. Security

Security on our ICT services is very important. If you discover a security problem, please inform the IT service provider, Eduthing, as soon as possible. Never demonstrate this problem to another user. All use of the ICT systems must be under your own username and password. Anyone found to be sharing accounts and passwords may have their access blocked. Any user identified as a security risk may have their access blocked and be subject to a disciplinary action.

5. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or any other networks that are connected to the system. This includes but is not limited to, uploading and/or creation of computer viruses, the wilful damage of computer hardware and deletion of data.

6. Electronic Mail & Messaging

An official email address will be provided to all staff members. This is the only email account which should be used to conduct work. Users are expected to use these services in a responsible manner. The sending of any emails that breach the terms of the IT User Agreement will result in disciplinary actions. Bulk sending of email without prior permission (spamming) is also forbidden.

7. Monitoring

All users email and system accounts have been provided to them by The School and should not be considered personal accounts. They are loaned to the individual for duration of the time at The School to undertake specific activities. The school reserves the right to monitor activity, using both automated systems (scanning for file types, file content) and manually.

Where there is sufficient reason to do so appropriate individuals will be granted access to the accounts.

.

8. Disciplinary Consequences

- If the rules of this Acceptable Use Policy are broken, users will have their computer privileges removed, this includes logon abilities, access to email and access to the internet. Depending on the severity of the issue one or more of the above restrictions may be implemented.
- If a staff member breaches the Acceptable Use Policy, any incident will be reported to the Headteacher for further action.

Acceptable Use: Workforce, Governors, Visitors and Volunteers.

The use of ICT resources must be in support of the role perform for The School. You are personally responsible for this provision at all times when you use any of the ICT resources.

By using any The School IT equipment after reading this ICT User Agreement means you understand and accept the terms and conditions detailed below Any breach of these conditions may lead to disciplinary proceedings.

i. I understand WhatsApp is not an approved communication channel for the school. As this is not a school-controlled platform, the school is not able to monitor or easily access the information held. This can cause issues if there were to be a Subject Access or Freedom of Information Request. The approved communication channels are school email, parent mail, and Microsoft Teams.

ii. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

iii. My passwords will be "strong" in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If I suspect it has been compromised, then I will change it immediately.

iv. I will ensure that I am the only one who uses my user Account and understand that anything undertaken while I am logged in, I will be held responsible for.

v. I will not autosave my password or log in details for any the School systems, as this negates the effectiveness of the password.

vi. I will lock my computer screen whenever I leave it unattended.

vii. I will ensure that all electronic communications are compatible with my professional role.

viii. If I receive a suspicious email, I will report it before clicking on any links, downloading any attachments or entering my user details. When I report it, I will not forward the email but send a screen shot.

ix. My personal social media accounts will not show a direct link with the school, and I understand that whatever I post can be seen, therefore if I am identifiable content will be of a professional nature.

x. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

xi. I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs. Under no circumstances should the operating system or installed applications on any school provided devices be modified by the user in any way.

xii. I will always check if I should be cc'ing bcc'ing recipients and that the correct email address, and attachment has been selected.

xiii. I will transfer personal data by email securely e.g., using egress, or password protecting it. The password will be sent in a sperate email.

xiv. I understand that anything I write in an email or document about an identifiable person can be requested via a Subject Access Request and read by that individual. Therefore, would not write anything that I would not want that person to read, could bring the organisation in disrepute or is counter to the staff code of conduct.

xv. I will consider if the communications I send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".

xvi. I understand that I can cause a Data Protection breach by destroying or corrupting data and all data should be held in line with The School's data retention schedule.

xvii. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

xviii. I will support the school's approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the organisation or its community' onto my own social media platforms.

xix. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Senior Leadership Team.

xx. I will respect copyright and intellectual property rights.

xxi. I will ensure that my online activity, both in work and outside work, will not bring The School my professional reputation, or that of others, into disrepute.

xxii. I will alert the school designated safeguarding lead if I feel the behaviour of any child may be a cause for concern.

xxiii. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated safeguarding lead.

xxiv. I will not use the School's ICT systems for any commercial activities, such as work for a for-profit organisation.

xxv. When using personal devices please ensure that the device has anti-virus in place that has been updated to limit potential vulnerabilities.

xxvi. We appreciate that others may use the personal devices you access the system with however please ensure that you are the only person who can access your user Accounts and that you understand that anything undertaken while you are logged in, will be considered done by you.

xxvii. will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.

School Workforce Only

I. I will only use the school's email (Microsoft Outlook), Internet, Intranet, and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governors.

II. I will ensure personal data is kept secure and is used appropriately, whether in the school, or when working remotely. Personal data should be stored on the R drive.

III. I will only access school resources remotely (such as from home) through Freedom2Roam (a service for LGfL National Grid for Learning community) and follow e-security protocols to interact with them.

IV. I will not install any hardware or software without the permission of the IT service provider, Eduthing.

Governors Only

- Local Governing Committee documentation is stored electronically on Governor Hub or securely in hard copy in line with the School's Document Retention Policy. Personal copies of documents should be retained in line with the school data retention schedule.

- Any information downloaded from the shared portal onto a personal device should be deleted upon completion of the task, including from the temporary internet files.

- Only School provided email accounts should be used for school business. This prevents subject access requests to personal email accounts and facilitates compliance with any email retention period. Please note that this email account can be monitored by appropriate individuals if there is due cause.

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	