

Online safety policy

Peters Hill Primary School



Approved by:	Mrs I Gilhooley	Date: 11.9.2023
Last reviewed on:	January 2023	
Next review due by:	September 2023	

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents/carers about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school	8
10. How the school will respond to issues of misuse	9
11. Training	9
12. Monitoring arrangements	10
13. Links with other policies	10

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 headteachers and school staff](#)
- [Relationships and sex education](#)

➤ [Searching, screening and confiscation](#)

It also refers to the DfE'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](#) 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.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 governing board 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 governing board 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 lead (DSL).

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

The governing board 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 board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support 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.

The governor who oversees online safety is Nick Foley

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 that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (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:

- › Supporting the executive headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the executive headteacher and governing board 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 headteacher, ICT manager 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 child protection policy
- › Ensuring that any online safety incidents are logged (see appendix 5) 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 governing board
- › 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, in order 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 manager (RM)

The ICT manager 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 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 continual 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 (see appendix 5) 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

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 that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that 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 informing the DSL immediately who will then take appropriate action with IT technicians and RM.
- Following the correct procedures by discussing with the Executive Headteacher/Associate Headteacher/DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

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:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That 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 home, and in information via our website and social media feeds. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What 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.

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. Class teachers will discuss cyber-bullying with their classes.

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

Pupils at Peters Hill do not have access to personal electronic devices within the school day, therefore any reports of inappropriate use to school staff will be referred to a parent to investigate.

If a child has ignored school rules and has access to their device in the school day but is unwilling to give in their device a parent will be called to assist with obtaining the device. If a parent is uncontactable, the child will be isolated from other children until a parent can be available to assist.

The Executive Headteacher, or Associate Headteacher/Deputy in their absence, 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

The Executive Headteacher 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. However, we will always endeavour to view the material in conjunction with the parent as stated above.

If inappropriate material is found on the device, it is up to the Executive 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:

- **Not** 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](#)

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.

Peters Hill 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.

Peters Hill will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

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

Pupils in Year 6 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Pupils will hand devices into school staff each morning for safe storage and they will be returned at the end of the day. Pupils are not expected to use their phones on school property before or after school.

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 Business Manager.

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. 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 / 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 that involve 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 DSL and deputies 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 DSL logs behaviour and safeguarding issues related to online safety. All incidents are recorded on CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. 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 procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

**ICT Acceptable Use Agreement for Pupils - Nursery – Year 2
(Covering the child whilst in Nursery – Year 2 at Peters Hill Primary School)**

It is important that you read this agreement carefully. If there is anything that you do not understand, please ask.

The school has installed computers and provided Internet access to aid our learning. I understand that the school may check my computer files and monitor any Internet sites I visit. These rules will keep everyone safe and help us to be fair to others.

I agree that:

- ☐ I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.
- ☐ I will use the technology at school for learning.
- ☐ I will use the equipment properly and not change or delete someone else's work.
- ☐ I will not use personal portable hard drives, USB Sticks or other Storage Media.
- ☐ I will only e-mail people I know, or my teacher has approved.
- ☐ If I attach a file to an email, it will not include anything that I would not want my teacher to see or read or anything that is disrespectful
- ☐ I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.
- ☐ I will report any unpleasant material or messages sent to me. I understand this would be confidential and would help protect other pupils and myself.
- ☐ I will not download any programs or games on to the school computers or portable devices unless I have permission to do so.
- ☐ I will keep all liquids and foods away from any of the school's ICT Equipment
- ☐ I will always check with a responsible adult before I share or publish images or videos of myself, my friends or other people onto the internet.
- ☐ I will not make audio or video recordings of another pupil or teacher without their permission.
- ☐ When using sites on the internet, I will not give my name, home address, telephone/mobile number, unless my parent, carer or teacher has given permission.
- ☐ I will not pretend to be someone else or arrange to meet someone I do not know.
- ☐ I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.
- ☐ I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).



**I am aware of the CEOP report button and know when to use it.
I know anything I do on the computer may be seen by someone else.**

TO BE SIGNED BY A PARENT (THIS CONSENT COVERS YOUR CHILD WHILST IN NURSERY – YEAR 2)

I confirm that I have spoken to my child about the contents of the ICT Acceptable Use Policy in a way that is appropriate for their age.

CHILD'S NAME

CLASS

As a parent/carer of the above pupil, I give permission for my son/daughter to use the computer systems to access the internet and email. I am aware that the school will endeavour to take all reasonable steps to restrict access to unsuitable material to the internet. I have read the rules for responsible Internet use and understand that pupils will be held accountable for their own actions.

PARENT'S NAME

Signed

Dated

CONSENT MAY BE WITHDRAWN AT ANY TIME BY WRITING TO THE HEADTEACHER

ICT Acceptable Use Agreement for Pupils - Year 3 – Year 6 (Covering the child whilst in Year 3 – Year 6 at Peters Hill Primary School)

It is important that you read this agreement carefully. If there is anything that you do not understand, please ask.

The school has installed computers and provided Internet access to aid our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit. These rules will keep everyone safe and help us to be fair to others.

I agree that:

- ☐ I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.
- ☐ I will use the technology at school for learning.
- ☐ I will use the equipment properly and not change or delete someone else's work.
- ☐ I will not use personal portable hard drives, USB Sticks or other Storage Media.
- ☐ I will only e-mail people I know, or my teacher has approved.
- ☐ If I attach a file to an email, it will not include anything that I would not want my teacher to see or read or anything that is disrespectful
- ☐ I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.
- ☐ I will report any unpleasant material or messages sent to me. I understand this would be confidential and would help protect other pupils and myself.
- ☐ I will not download any programs or games on to the school computers or portable devices unless I have permission to do so.
- ☐ I will keep all liquids and foods away from any of the school's ICT Equipment
- ☐ I will always check with a responsible adult before I share or publish images or videos of myself, my friends or other people onto the internet.
- ☐ I will not make audio or video recordings of another pupil or teacher without their permission.
- ☐ When using sites on the internet, I will not give my name, home address, telephone/mobile number, unless my parent, carer or teacher has given permission.
- ☐ I will not pretend to be someone else or arrange to meet someone I do not know.
- ☐ I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.
- ☐ I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).



**I am aware of the CEOP report button and know when to use it.
I know anything I do on the computer may be seen by someone else.**

CHILD'S NAME

CLASS

Pupil's Signature

TO BE SIGNED BY A PARENT (THIS CONSENT COVERS YOUR CHILD WHILST IN YEAR 3 – YEAR 6)

I have discussed the ICT Acceptable Use Policy for Pupils with my child and confirm that he/she has understood what the rules mean.

As a parent/carer of the above pupil, I give permission for my son/daughter to use the computer systems to access the internet and email. I am aware that the school will endeavour to take all reasonable steps to restrict access to unsuitable material to the internet. I have read the rules for responsible Internet use and understand that pupils will be held accountable for their own actions.

PARENT'S NAME

Signed

Dated

CONSENT MAY BE WITHDRAWN AT ANY TIME BY WRITING TO THE HEADTEACHER

ICT Acceptable Use Policy

This policy applies to all adult users of the school's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the School Business Leader or IT Technician. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return to school.

Please also refer to the school's Information and Cyber Security Policy, Data Protection Policy and Password Policy, along with Staff Code of Conduct, Keeping Children Safe in Education and Guidance for Safer Working Practices.

Any inappropriate use of the School's computer, internet or e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being breached or abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or access to the internet and electronic systems. All information relating to our pupils, parents and staff is personal. It can take many forms and includes, but is not limited to, paper (written, printed), electronic, communications. Such information is protected under the Data Protection Act 2018 and General Data Protection Regulation (UK GDPR). You must treat all school information with the utmost care, however held, and ensure information is secure at all times.

Official school systems must be used when processing and/or accessing information.

All liquids and foods must be kept away from any of the school's ICT Equipment, as damage from these can cause serious implications to the equipment and is costly to repair.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. The Computer Misuse Act 1990 makes it an offence to access any computer system to which you do not have an authorised right to use. For your information, the following activities are examples of criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking
- unauthorised modification of computer material
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:

- If you download any image, text or material check if it is copyright protected. © identifies copyright protection. Only non-copyright materials, images, texts etc should be used unless permission from the owner is sought. Speak to the Admin Manager if you require further guidance.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to the Headteacher.
- Do not download any software or apps onto school systems or devices.

- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

You should not:

- introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- seek to gain access to restricted areas of the network;
- knowingly seek to access data which you are not authorised to view;
- introduce any form of computer viruses;
- carry out other hacking activities
- undertake any other activities deemed illegal under the Computer Misuse Act 1990.

School devices will access school Wi-Fi and internet. Access to school Wi-Fi and internet is to be used for school business or professional development only. School Wi-Fi should not be accessed for personal use.

With reference to Guidance for Safer Working Practices, it is advised that staff should disable internet access, mobile data, and data transfer facilities/apps, on personal devices and mobile phones, when entering school premises.

Personal devices and mobile phones should not be used during working hours for personal use.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

- providing evidence of business transactions;
- making sure the School's business procedures are adhered to;
- training and monitoring standards of service;
- preventing or detecting unauthorised use of the communications systems or criminal activities;
- maintaining the effective operation of communication systems.

In line with this policy the following statements apply:

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Emails containing sensitive personal data should be encrypted. This can be done by typing ENCRYPTED: at the beginning of the subject line. If you need guidance on how to do this please speak to the IT Technician.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, or offensive comments or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

- It is good practice to re-read e-mails before sending them as external e-mail cannot be retrieved once they have been sent. This should include checking the email is going to the correct recipient, as sending emails to an incorrect recipient may be deemed as a data breach.
- School internet and e-mail access is intended to be used for school business or professional development only. As such, they should not be used in a personal capacity.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.
- Be aware that there are many ways in which malicious intent and actions by others could affect you and/or the school. Some of these include, but are not limited to:
 - Phishing – this is where emails appear to be from a legitimate source but may ask you to reveal information to be used for fraudulent activities, e.g. requesting account details.
 - Spam – also known as junk emails. These are unsolicited messages sent to attempt fraudulent activities such as the promotion of non-existent products.
 - Similar to the previous points, criminals can send emails which contain attachments or links that they ask you to open or click on. When doing so this can cause malicious effects to networks, email accounts etc. Such links or attachments should not be opened.
 - If you suspect you are in receipt of any phishing, spam or suspicious email, inform the IT Technician immediately.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites. Internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia and Google Sites
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter, Instagram

When using school approved social networking sites, the following statements apply:

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @petershillprimary.org email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright or data protection or other claims.

This includes, but is not limited to, material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a child or vulnerable adult at risk of harm.
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them.
- When posting images/videos of children, do not include any names in titles, captions or descriptions
- Content or use should not breach any relevant school policy.

Data protection

The processing of personal data is governed by the Data Protection Act 2018 and General Data Protection Regulation (UK GDPR). Schools are defined in law as separate legal entities for the purposes of complying with the UK GDPR. Therefore, it is the responsibility of the School to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the school in line with appropriate policies. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work, personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the school's premises or working remotely, you must:

- keep the data secure and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask the Head Teacher or School Business Leader;
- familiarise yourself with the provisions of the UK GDPR and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the school holds on them subject to any exemptions that may apply

When personal data is collected, stored or processed, on school systems, the data must be appropriately secured and protected in line with school policies. Please also refer to the school Password Policy.

Personal data should not be stored or downloaded directly onto any portable devices. Should any personal data be inadvertently downloaded to a portable device, it must be securely deleted from the device, in line with school policy. In this instance, inform the IT Technician immediately.

Personal data storage on removal media is not allowed, even if that media is encrypted.

Staff are to use school storage solutions only, such as Office 365 (SharePoint and OneDrive), Integris, and must not use personal portable hard drives or USB Sticks.

If you make, or encourage another person to make, an unauthorised disclosure knowingly or recklessly, you may be held criminally liable and/or be subject to disciplinary proceedings, not excluding dismissal.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:

PRINT NAME:

Dated: