Flourishing together

Policy: On-line Safety
Subject leader: Lauren Hayton

Introduction
This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

This policy should be read in conjunction with the St Peter's policies for:
Teaching and Learning
Positive Behaviour Management
Safeguarding
Remote learning policy

1. St Peter's C of E Primary School: Vision for Online Safety

St Peter's C of E Primary School provides a diverse, balanced and relevant approach to the use of technology where children are encouraged to maximize the benefits and opportunities that technology has to offer. We ensure that the children in our care learn in an environment where security measures are balanced appropriately with the need to learn effectively and equip them with the skills and knowledge to use technology appropriately and responsibly. Our children are taught how to recognise risks associated with technology and how to deal with these risks both within and outside the school environment. We work with all members of our school community to educate them about the risks associated with technology and need for a school Online Safety policy.

2. St Peter's Online Safety Champion.

Our Online Safety Champion is the Computing Subject Leader in partnership with the Senior Leadership Team.

At St Peter's C of E Primary School, the role of the Online Safety Champion includes:

Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policy (see appendix 1).

- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring that all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up to date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP)
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.

- Ensuring the Headteacher/SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Safeguarding Lead to ensure a coordinated approach across relevant safeguarding areas.

3. **Security and data management**

ICT/Computing is a complex subject that involves all technology users in school, dealing with issues regarding the collection and storage of data through the physical security of the equipment. We ensure that procedures are in place to ensure data, in its many forms, is kept secure within our school. Where sensitive or personal data is recorded, we ensure that it is processed and transferred in line with the requirements of the EU General Data Protection Regulation (GDPR 2018). We ensure that this data is:

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

All data in our school is kept secure and staff are informed of what they can and cannot do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP).

4. Use of mobile devices

St Peter's C of E Primary School uses a range of mobile devices, including laptops, tablets, mobile phones and cameras. Whilst these provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of Online Safety. Many of these devices integrate functionality to take images, access the internet and engage users in various methods of external communication. Staff are aware that some mobile devices can access unfiltered internet content.

4.1 Mobile phones

Mobile phones can present a variety of challenges if not used appropriately. St Peter's C of E Primary School sets clear boundaries for their use in school.

- Adults are not permitted to use personal mobile phones during lesson time or at any point where they are involved in the teaching or supervision of children. During directed time, mobile phones should normally be switched off. If staff need to use their phone for lessons authorisation from SLT is needed.
- Adults may use personal mobile phones on site at other times.
- Year 6 children who have permission to bring mobile phones to school are required to hand them to a member of their class staff team at the beginning of the school day, named. They may collect them at the end of the day. Children should switch off their mobile phone before

entering the school grounds and handed in and it should remain switched off and out of sight until they have left the school grounds.

- St Peter's C of E Primary School recommends that personal mobile phones are security marked, password protected and insured, although this is not a requirement.
- All staff, visitors or children can be contacted through the school office in the event of an emergency.
- Images, video or audio must not be recorded on personal mobile phones.
- Staff are permitted to access the internet via personal mobile phones using the school's wi-fi network within the guidelines of the school's Acceptable Use Policy.
- A "school mobile" will soon be available for staff to use whilst outside the building on school trips. This is for "business use" only. It is the responsibility of the school office staff to ensure that this device is fully charged, in credit and ready for use.
- The acceptable use of mobile phones by visitors to school, including parents, is made clear in the Safeguarding Policy and the Acceptable Use Policy signed by all visitors.
- Staff are aware that mobile phones could be used in cyberbullying. The dangers of cyberbulling are taught directly in our school through the Kidsafe program and through the Computing and PSHE curriculum.
- Staff are aware that they may confiscate any phone or device. There are guidelines from the DFE in the Safeguarding Policy regarding the confiscation of property.
- Staff are asked to be vigilant in monitoring visitors for any covert use of mobile phones or cameras.
- Any member of staff who is concerned about suspicious use of mobile phones or cameras should report them to the DSL.

4.2 Other mobile devices

- Children are not permitted to bring other mobile devices into school.
  Adults who bring personal tablet devices into school are subject to the advice outlined above and to the school's Acceptable Use Policy.
- During the course of learning within school staff may take images of children as a record of an activity or trip or as part of ongoing assessment.
- Parental consent is obtained to take and use photographs and/or videos of children, for use in school, to market the school or to share on social media/internet.
- When taking photographs, staff are required to ensure that all photographs are dealt with appropriately and sensitively.

4.3 Parents Taking Photographs/Videos

- Under the Data Protection Act (1998) parents are entitled to take photographs of their own children on the provision that the images are for their own use. (There will be occasions when we kindly request that photographs will not be taken at events. This is to safeguard your children).

- Parents are informed at the beginning of events that they should only take photographs of their own children.
- Parents are reminded in writing each year, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable unless specific permission has been obtained from the subjects.

4.4 Storage of Photograph/Videos

- All images stored on cameras remain with school staff at all times.
- Images stored on tablets or using Cloud storage are kept securely and are password protected.
- All images stored on the above mentioned devices are downloaded to the photographs folder on the school server and then deleted from the device memory at the earliest possible occasion.
- Staff are not permitted to store images on personal devices.
- Staff are permitted to store personal images on school equipment. These are password protected.
- Photographs or videos stored on the school network are secure and password protected.

4.5 Publication of Photographs /Videos

- Written consent is gained from parents for publication of children's images through the school admissions form. Parents are made fully aware of how their children's images will be used and any personal information which could be attached to them.
- The school makes every effort to ensure that photographs are not available for downloading or misuse.
- Full names do not accompany published images.
- Staff receive training to raise their awareness and understanding of the risks associated with the publication of images, particularly in relation to the use of personal Social Network sites. Staff are strongly advised to ensure that personal profiles are secure and do not display content that is detrimental to their own professional status or could bring the school into disrepute. Additional required reading is appended to the school's staff handbook (available to download on the school's website)

4.6 The Media, 3rd Parties and Copyright

- In the event of 3rd parties taking, storing or transferring images whilst in school, the school will make itself fully aware of who owns the copyright for such images**.**

4.7 CCTV, Video Conferencing, VOIP and Webcams.

- School has 24hr CCTV externally and used for monitoring purposes. School does not currently make use of any other named technology above. If such a situation were to arise then use of these would be fully reviewed by the Online Safety Champion.

5. Communication Technologies

St Peter's C of E Primary School uses a variety of communication technologies to enhance the smooth running of the school. All staff are aware of the benefits and risks associated with this.

- All email users have access to the Office 365 service as the school's preferred email system.
- Staff are permitted to use their personal email accounts on school equipment but must use the school's preferred system for professional communications.
- Children do not currently have school email accounts.
- The BTLancashire Lightspeed Filtering service filters SPAM received. Any incidents of SPAM should be reported to the school Online Safety Champion and Headteacher and will then be referred to ISP.
- All staff are advised of the dangers of accessing content such as SPAM, phishing, unsuitable materials, and viruses from external email accounts, in school.
- All users are aware that email is covered by the Data Protection Act (1988) and the Freedom of Information Act (2000) meaning that safe practice should be followed in respect of record keeping and security. All staff and class email accounts are password protected.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- Any email which makes users feel uncomfortable, is offensive, threatening or bullying in nature should be reported to the Online Safety Champion and Headteacher.
- All users are made aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.
- All outgoing email communication from any email address ending @stpetersheysham.lancs.sch.uk contains a disclaimer at the bottom.

5.1 Social Networks

The school uses Facebook as a way of communicating with parents and the wider community. The school is aware that many staff use Social Networks on a personal level.

All staff are aware that on any social media they may use that:

No personal details should be shared with children via Social Networking sites.

- Privacy settings should be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Personal contact details should not be given to pupils, parents or carers including mobile telephone numbers, details of any blogs or personal websites.
- The content posted online should not:
  - Bring the school into disrepute
  - Lead to valid parental complaints
  - Be deemed as derogatory towards the school and/or its employees
  - Be deemed as derogatory towards pupils and/or parents and carers
  - Bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication may be considered inappropriate or misinterpreted.
- Communication via personal social media accounts with parents, past pupils, siblings of pupils, especially if under the age of 18 is discouraged.
- Children associated with the school, must not be added as "friends" on any Social Network site.

The school advises parents that:

- Posting inappropriate comments about staff or children could be construed as instances of cyberbullying.
- They should not posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

5.2 Instant Messaging or VOIP

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher. St Peter's C of E Primary School chooses to block all social networking sites.

Through teaching or staff training:

- Staff and children aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts?
- Staff may use school equipment to communicate with personal contacts outside of directed time e.g. through 'Facetime' on an iPad?
- The school text messaging service (Teachers 2 Parents) is protected by a SSL 128 bit certificate. All Teachers 2 Parents staff have CRB clearance and they are fully compliant with the Data Protection Act.

5.3 St Peter's C of E Primary School Website

From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website. St Peter's C of E Primary School is fully compliant with this.

The school:

- Uses its website to Communicate Online Safety messages to parents/carers.
- Makes staff aware of the guidance regarding the inclusion of personal information on the website/ online publication?
- Enables all staff to edit online publications and requires class teachers to ensure that the content is relevant and current.
- Protects some content in a password protected area.
- Ensures that downloadable materials are in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

5.4 Showbie as a Remote Learning Platform during COVID-19

This section of the policy will be enacted in conjunction with the school's Remote Learning Policy.

In the event of a class or the whole school needing to move to remote learning during the COVID-19 pandemic, the school uses the learning platform Showbie. This platform has been specifically created for use in schools.

- The platform is fully password protected and all content is held securely. Children and staff must have a secure log in to access any content on Showbie.

- In order to join a class on Showbie and access class content, parents need to create a secure log in for their child and enter a unique code given by the school.
- Teachers have to approve any requests for individuals to join their class.
- Staff have access to information provided by parents when creating their child's log-in. All staff are fully compliant with the Data Protection Act.
- Children's access to the platform is restricted to the work set for them.

- The platform allows staff to:
  - Set work for pupils in the event of remote learning
  - View any work completed and submitted by pupils
  - Provide written feedback on learning

The school advises parents that:

- Children are supervised when using Showbie and accessing online materials.
- Any communication with teachers via Showbie is carried out by parents, rather than children.

6. Infrastructure and technology

The school ensures that the infrastructure/network are as safe and secure as possible. St Peter's C of E Primary School subscribes to the BT Lancashire Service and internet content filtering is provided by default.

- It is noted that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.
- Sophos Anti-Virus software is installed on computers in school and configured to receive regular updates.

6.1 Children's access

- Children are supervised when accessing school equipment and online materials.
- All children are provided with individual logins.
- Children's access is restricted to the Pupils Documents (M:) drive and the Shared Area (Z:) on the network.

6.2 Adult access

- All classroom staff have access to information held on the curriculum drives. Access to admin drives is restricted to the head teacher and office staff. This is held on a separate server to the main network server. All children are provided with individual logins.
- Limited access is available to supply teachers through separate logins.

6.3 Passwords

- All classroom staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools.
- All users of the school network have a secure username and password.
- The administrator password for the school network is available to the head teacher, computing subject leader and IT technician.

- Staff and children are reminded regularly of the importance of keeping passwords secure.

6.4 Software/hardware

The school has legal ownership of all software.

- An up to date record of appropriate licenses for all software and is maintained by the IT technician.
- The IT technician, in communication with the Computing subject leader, regularly audits equipment and software
- The IT technician, together with the head teacher and Computing coordinator control what software is installed on school systems.

6.5 Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have security enabled.
- Wireless networks are accessible only through a secure password.
- Access settings have been restricted on tablet devices.

The ICT technician, in partnership with the head teacher, is responsible for managing the security of our school network.

- School systems are kept up to date in terms of security.
- All users of the school network have clearly defined access rights to the school network through their username and password.
- Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended.
- The IT technician is responsible for installing new software.
- All users should report any suspicious activity or evidence of a breach of security to the head teacher or Online Safety Champion.
- Cloud storage of school documents is recommended to staff but the school recognises that some staff use removable storage devices e.g. encrypted pen drives.
- Teachers may not use their school laptop or iPAD (if they have one) for personal or family purposes.
- Any network monitoring which takes place is in accordance with the Data Protection Act (1998) and GDPR (2018).
- All internal/external technical support providers are aware of our schools requirements / standards regarding Online Safety.
- The head teacher and Online Safety Champion are responsible for liaising with/managing the technical support staff.

6.6 Filtering and virus protection

- The school has requested devolved control over the BT Lancashire filtering service(Lightspeed Rocket) and this is now managed by the head teacher and the IT technician when authorised by the head teacher.
- Information regarding devolved filtering is stored on the Lightspeed website.

- The IT technician ensures that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school. He does this by requesting such equipment from individual staff when updates are required. A log is kept.
- Staff report suspected or actual computer virus infection to the computing subject leader and IT technician.

7. Dealing with incidents

An incident log (see Appendix) is completed to record and monitor offences. This is audited on a regular basis by the head teacher, Online Safety Champion and other members of the Senior Leadership Team.

7.1 Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

The school will **never personally investigate, interfere with or share evidence. It is aware that were it to do so it may inadvertently be committing an illegal offence.**

All illegal content will be reported to the Internet Watch Foundation (**http://www.iwf.org.uk**).

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

7.2 Inappropriate use

It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Incident Procedure and Sanctions	
Using other people's logins and passwords maliciously.	Inform Head teacher or Online Safety Champion.
Deliberate searching for inappropriate materials.	Enter the details in the Incident Log. Additional awareness raising of Online Safety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

- The head teacher and/or Online Safety Champion are responsible for dealing with Online Safety incidents.
- All staff are aware of the different types of Online Safety incident and are aware that these should be reported to the head teacher or Online Safety Champion.

- Procedures for dealing with these are outlined above.
- Children are aware of what to do should they accidently access inappropriate material.
- Incidents are logged in the Online Safety Incident Record.
- Incidents are monitored by SLT, termly.
- Parents and/or external agencies are involved if the incident raises a Child Protection concern or relates to bullying.

The 'Online Safety Incident/ Escalation Procedures' document (See Appendix) is used as a framework for responding to incidents.

8. **Acceptable Use Policy (AUP)**

St Peter's C of E Primary School's Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are for Staff and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. This agreement is to ensure that users are kept safe when using technology.

The AUP for children is displayed in each classroom as the expected behaviour for staying safe with ICT

For a copy of the St Peter's C of E Primary School AUPs: see Appendix

9. Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that the use of technology can provide. However, St Peter's C of E Primary School considers it essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond.

St Peter's C of E Primary School considers that the four main areas of Online Safety risk to be aware of and consider are:

- Content – being exposed to illegal, inappropriate or harmful content
- Contact – being subjected to online interaction with other users. This could be peer to peer pressure, commercial advertising or adults posing as children.
- Conduct – personal online behaviour that increased the likelihood of, or causes, harm
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

We teach our children to:

- be able to communicate safely and respectfully online,
- be aware of the necessity to keep personal information private,
- be taught how to search effectively
- be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.
- be aware of who to talk to should they have any worries or concerns regarding online safety

Area of Risk	Example of Risk
Content: Children and staff need to be aware that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), • substance abuse. • Lifestyle websites, for example proanorexia/ self-harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children and staff need to be aware that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming Cyberbullying in all forms, including peer-on-peer abuse Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children and staff need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, indecent images, digital footprint and online reputation • Health and well-being - amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images). • Copyright (little care or consideration for intellectual property and ownership – such as music and film).
Commerce: Children and staff need to be made aware that contact may be made by companies/individuals aiming to cause financial harm/data theft, and the importance of protecting personal information.	• Online gambling • Inappropriate advertising • Phishing • Financial scams

(Ofsted, 2013, Inspecting Online Safety – guidance document

9.1 Peer on Peer Abuse

St Peter's C.E Primary School recognises that children are vulnerable to and capable of abusing their peers. This can happen through mobile and smart technology, otherwise called 'cyberbullying'. We take such abuse as seriously as abuse perpetrated by an adult. This includes verbal as well as physical abuse. Peer on peer abuse will not be tolerated or passed off as part of "banter" or "growing up".

We recognise that peer on peer abuse can manifest itself in many ways such as:

• Child Sexual Exploitation
• Sexting or youth produced digital imagery
• Upskirting
• Bullying
• Radicalisation
• Abuse in intimate relationships
• Children who display sexually harmful behaviour
• Technology can be used for bullying and other abusive behaviour

We are committed to a whole school approach to ensure the prevention, early identification and appropriate management of peer on peer abuse within our school and beyond. In cases where peer on peer abuse is identified we will follow our child protection procedures, in line with the school's Child Protection and Safeguarding Policy, taking a contextual approach to support all children and young people who have been affected by the situation.

9.2 Indecent Images Shared by Children

This section of the policy will be enacted in conjunction with the school's Child Protection and Safeguarding Policy. 'Youth produced sexual imagery' or 'sexting' is the production and/or sharing of sexual photos and videos of and by young people under the age of 18. This is not include the sharing of sexual photos/videos of under 18s by adults. This is a form of child sexual abuse and must be referred to the police.

The school will ensure that:

- Staff are aware that the sharing of indecent imagery is a safeguarding concern
- Staff receive appropriate training regarding sexting in the school community
- Staff are aware that creating, possessing, and distributing indecent imagery of children is a criminal offence
- Should a member of staff become aware of an incidence of sexual imagery, the correct safeguarding procedures are followed, as sited in the school's Safeguarding Policy.

9.3 Online Safety - Across the curriculum

St Peter's C of E Primary School believes it is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' Online Safety.

We seek to provide relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement. Regular, planned Online Safety teaching is provided throughout the school through the Kidsafe program and through the computing curriculum. Online Safety teaching is delivered to our EYFS children, at an age appropriate level. Online Safety education is differentiated for children with special educational needs as outlined in the individual child's provision maps or Care Plan.

Online Safety teaching for children will:

- Be delivered in line with the guidance and recommendations in KCSIE (2021)
- Ensure that children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998), GDPR (2018) and copyright implications?
- Make children aware of the impact of cyberbullying and how to seek help if they are affected by these issues.
- Teach children to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- Ensure that children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Remind children of safe Internet use.

The impact of this training will be monitored by the Online Safety Champion Coordinator as part of the school's curriculum monitoring.

Online Safety – Raising staff awareness

Online Safety training for all teaching and non-teaching staff, to ensure they are regularly updated on their responsibilities, is provided at least annually. The head teacher and Online Safety Champion (Lauren Hayton) will provide advice/guidance to all staff when needed. The Online Safety Champion will receive Online Safety training/updates as provided by LCC.

Staff training will:

- Ensure that staff are made aware of issues which may affect their own personal safeguarding.
- Make it clear that staff are expected to promote and model responsible use of ICT and digital resources.
- Be provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.

Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues will be discussed in staff meetings.

Online Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often

unsure about what they would do about it.” (Byron Report, 2008) The school seeks to assist parents in protecting children online through:

- Promotion of external Online Safety resources/online materials through the school website
- By holding annual Safer Internet workshops for parents.

Online Safety – Raising Governors awareness

The Online Safety Policy is regularly reviewed and approved by the governing body.

Signed on behalf of the Governing Body	Bridget Longdon
Date	January 2021
Review Date	January 2022

Appendix 1 – AUP’s

Flourishing together

St Peter's C of E Primary School Acceptable Use Policy (AUP) – Staff

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff are aware of their individual responsibilities when using technology. All staff members are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during directed time.
9. I will not install any hardware or software without the prior permission of the headteacher or IT technician.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network, or lock my workstation, when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agreed to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

Full Name …… (PRINT)

Position/Role ……

Flourishing together

On-line safety Rules

KS2

1. We always ask permission before using the Internet and ensure a trusted adult is around while we use it.
2. We immediately close/minimise any page we are uncomfortable with and tell a responsible adult if we see anything we are uncomfortable with.
3. We only communicate online with people a trusted adult has approved.
4. All our online communications are polite and friendly.
5. We never give out our own or others' personal information or passwords and are very careful with the information that we share online.
6. We only use software approved by a trusted adult
7. We will not use any personal devices in school unless approved by a trusted adult.

I have read these rules and agree to follow them at all times whilst in school.

Signed _____ Date: _____

On-line safety Rules

KS1 and Early Years

1. We only use the Internet when a trusted adult is around.
2. When we talk to people using computers, we are always polite and friendly.
3. We always make careful choices when we use the internet.
4. We always ask a trusted adult if we need help using the Internet.
5. We always tell a trusted adult if we find something that upsets us.
6. We will only click on buttons if an adult has said its okay to do so.

I have read these rules to my child and they understand that we must follow them at all times whilst in school.

Signed (parent/guardian on behalf of child): _____

Date: _____

Flourishing together

ST PETER'S C. OF E. PRIMARY SCHOOL

AUP for users of St. Peter's Technology

September 2021

To be signed by any adult working in our school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

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

3. I will not use any external device to access the school's network e.g. pen drive.

4. I will respect copyright and intellectual property rights.

5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and only with permission from the Headteacher. I will not distribute images outside the school network without the prior permission of the Headteacher.

6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

8. I will not install any hardware or software onto any school system.

9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

I have read and agree to follow this code of conduct and to support the safe use of technology throughout the school.

Print name: _____

Signed: _____ Date :