St Peter & St Paul School

Policy last reviewed	October 2022
Next Review	September 2024
Review initiated by	Headteacher

ONLINE SAFETY POLICY

At St Peter & St Paul School we will develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices as they develop their personalised learning, in line with our school's vision.

Network Management Company: NXControl

Online Safety Lead: Hayden Mather, NXControl

Online Safety Co-ordinator / DSL: Scott Nixon

Contents

Appendices

1.0 Introduction

It is the duty of St Peter & St Paul School to ensure that every pupil in its care is safe and the same principles apply to the digital world as apply to the real world. We recognise that IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people.

As a result of this, our pupils are taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities.

Current and emerging technologies used in and outside of school include, but are not limited to: Websites; Email and instant messaging; Blogs; Social networking sites; Chat rooms; Music / video downloads; Gaming sites; Text messaging and picture messaging; Video calls; Podcasting; Online communities via games consoles; Smart Watches Mobile internet devices such as smart phones and tablets; and Home internet devices such as computers and Smart televisions.

This policy, supported by the Acceptable Use agreements for staff and visitors and Charters for pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

It is linked to the following school policies and documentation:

- Safeguarding and Child Protection Policy (KCSiE)
- Anti-Bullying Policy
- Behaviour Management, Discipline & Exclusions Policy
- Staff Code of Conduct
- Health and Safety Policy
- Acceptable Use agreements and Charters
- Privacy Policy
- The PSHEE and Computing Curriculum.

We recognise that IT is generally considered both exciting and beneficial in and out of the context of education, however we also note that much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Peter & St Paul School, we understand the responsibility to educate our pupils on online-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online-safety and listening to their fears and anxieties as well as their thoughts and ideas.

2.0 Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. All users need to be aware of the range of risks associated with the use of these internet technologies.

In this policy:

- 'Staff' includes any person working in the school including teaching and non-teaching staff, trustees, visiting Peripatetic teachers and regulated volunteers.
- 'Parents' includes pupils' carers and guardians.
- 'Visitors' includes anyone else who comes to the school, including supply teachers, occasional volunteers and contractors.

Both this policy and the Acceptable Use Agreements / Charters (for all staff, visitors and pupils) cover, but are not limited to, fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, screens, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches etc.).

3.0 Roles and Responsibilities

3.1 The Trustee Board

The Trustee Board of the school is responsible for the approval of this policy and for reviewing its effectiveness.

3.2 Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community, and this includes responsibility for online-safety in conjunction with the online-safety lead and the DSL/online-safety co-ordinator. The Headteacher works with the Designated Safeguarding Lead/Online-Safety Co-ordinator, the Online-Safety Lead and the Network Management Supplier to ensure the day-to-day compliance in relation to e-safety.

In particular, the role of the Headteacher and the Senior Leadership team is to ensure that:

- staff, in particular the DSL / Online-Safety Co-ordinator and the Online-Safety Lead, are adequately trained about online-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online-safety in connection to the school.

3.3 The DSL/ Online-Safety Co-ordinator and Online-Safety Lead

The Online-Safety Lead and the Online-Safety Co-ordinator/DSL are responsible to the Headteacher for the day to day issues relating to e-safety. They will work with the school's network management company and the School Business Manager to ensure this policy is upheld by all members of the school community. They will keep up to date on current online-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the **Derby and Derbyshire Safeguarding Children Partnership**.

3.4 Network Management Company

The school's Network Management Company is responsible for maintaining a safe technical infrastructure at the school. They will provide advice to the school to keep St Peter & St Paul School abreast with the rapid succession of technical developments, to ensure the security of the school's hardware system and its data, and for training the school's teaching and administrative staff in the use of IT.

The Network Management Company will maintain the filtering system and any inappropriate usage will be reported to the Headteacher and Online-Safety Co-ordinator/DSL and dealt with in line with the Disciplinary Procedure for staff or the Behaviour Management, Discipline and Exclusion Policy for pupils.

3.5 Teaching and support staff

All staff are required to read the school's Online-Safety policy, the staff code of conduct and sign the Staff Acceptable Use Agreement before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online-safety issues which may arise in classrooms on a daily basis.

Staff must report any suspected misuse or problems to the DSL or Headteacher.

3.6 Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Charter, and for letting staff know if they see IT systems being misused.

Parents of children in Year 1 and 2 are required to sign the pupil Acceptable Use Agreement to acknowledge they have discussed this with their child. From Years 3-6, children and their parents will be expected to sign the Pupil Acceptable Use Agreement annually before being given access to school systems. Signed Acceptable Use Agreements will be held for 1 year.

All children will follow an online-safety course at the beginning of each academic year during their computing lesson or pastoral time and they will discuss the 'Acceptable Use Charter' and what it means. They will all be asked to sign a charter which will be displayed in their classrooms and the computer room.

3.7 Parents and carers

St Peter & St Paul School recognises that it is essential for parents and carers to be fully involved with promoting e-safety both in and outside of school.

The school will provide guidance to parents in the Parent Handbook and provide updates in relation to e-safety as necessary, seeking to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Charter.

4.0 Education and training

St Peter & St Paul School recognises the importance of education and training in relation to online-safety for both employees and children.

4.1 Staff: awareness and training

New staff at St Peter & St Paul School receive information on the school's e-Safety Policy and will be expected to sign an Acceptable Use Agreement as part of their induction.

All staff receive regular information and training on online-safety issues in the form of INSET training and during internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online-safety.

Any visitors using the school's IT resources should read the online-safety policy and sign the Acceptable Use Agreement.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate online-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

Any concerns regarding online-safety should be reported to the DSL, Online safety Lead or Headteacher. The DSL will keep a record of all online safety incidents and concerns.

4.1.1 Using IT to teach remotely

With the advent of remote teaching, it is important that staff follow the guidelines as outlined in the Child Protection and Safeguarding Policy and any interim guidance as applicable. Staff should as a matter of course:

- If 1:1 tuition is essential (e.g., peripatetic lessons, 1:1 SEND lessons), staff must seek agreement from the Headteacher and the pupil's parent. The parent is expected to be present throughout the lesson, or if this is not possible, the lesson should be recorded.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Where staff are working remotely any technology used for communication should be in appropriate areas and staff need to be mindful that the background does not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
- Live classes should be kept to a reasonable length of time and the timings shared with parents and pupils to ensure that children receive frequent breaks from the 'screen'.
- St Peter & St Paul School reserves the right for staff members to record live streamed sessions with pupils as a log of the activity. Parental approval will be sought. The purpose of any potential recording of live sessions would be so that the video can be reviewed if any issues were to arise.
- If live streams are to be recorded, this should be reflected in communication with staff, parents and children and agreement sought.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by the SLT and approved by our IT network provider to communicate with pupils.
- Emails must not be sent to a child's personal account – all communication should go through parents or generically through the Teams Channel.
- Staff should record attendance at online lessons. If a child expected to join an online lesson is absent the school office must be informed.

4.2 Pupils: Online Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for online-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried

out through PSHEE lessons, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online-safety responsibilities and to look after their own online safety. Pupils can report concerns to the Designated Safeguarding Lead, and any member of staff at the school.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. Pupils should approach the Designated Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Pupils should be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

4.3 Parents

The school seeks to work closely with parents and carers in promoting a culture of online-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and carers may feel equipped to protect their son or daughter when they use electronic equipment at home.

If necessary, we will arrange information sessions for parents or send out suitable material / recommended websites if we need to share advice or good practice with the parent body which will provide information about the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Publications and guidance for parents will be sent home as appropriate.

5.0 Policy Statements

5.1 Use of school and personal devices in relation to the safety of others

5.1.1 Staff

School devices assigned to a member of staff as part of their role must have a password so that unauthorised people cannot access the content. **When they are not using a device staff must ensure that it is locked to prevent unauthorised access**.

Staff at St Peter & St Paul School are permitted to bring in personal devices for their own personal use. Staff are not allowed to use their personal devices while with children (except in emergencies, while on the Sports

Field or off-site if a school mobile is not available) or at any time within the Early Years setting. They may use such devices only during break-times, lunchtimes, non-contact lessons or before/after the school day. Personal devices should be kept in lockers, drawers or in handbags during lessons.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils and only with parents if unrelated to school business. Under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system for anything related to school business, unless in an emergency, with permission from the Headteacher.

5.1.2 Pupils

Pupils must not bring mobile devices into school, unless they have been given permission by the Headteacher. Any devices brought into school must be handed in to Reception at the start of the day and collected when they leave school. These requirements apply to phones and all devices that communicate over the internet.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENDCo and / or Headteacher to agree how the school can appropriately support such use. The Headteacher will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

6.0 Use of Internet and Email

6.1 Staff

Staff must not access social networking sites or any website or personal email which is unconnected with schoolwork whilst in front of pupils. Such access may only be made during break-times, lunchtimes, non-contact lessons or before/after the school day and only on personal devices.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that all internet usage through the school network and staff email addresses is monitored.

Staff must immediately report to the DSL and/or Online-Safety Lead the receipt of any communication that makes them feel uncomfortable, is

offensive, discriminatory, threatening or bullying in nature or a communication which comes from an unknown, or potentially untrustworthy source. Staff must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Network Management Company and where appropriate, the DSL.

Staff should not respond directly to an email sent to them from a pupil's email account. Any response should be sent to the parent's email account and the parents informed.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring St Peter & St Paul School into disrepute;
- breach confidentiality;
- breach data protection legislation;
- carry out an action which is unlawful;
- or do anything that could be considered discriminatory against or bullying or harassment of any individual in the school.

Under no circumstances should school pupils be added as social network 'friends' or contacted through social media or personal email by any member of staff.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a parent / carer using their personal email address unless for non-school related business. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

6.2 Pupils

Our network has in place multiple layers of security to make sure pupils are working within a safe environment when using computer systems, they include but are not limited to Anti-Virus (managed and monitored), Boundary Firewall, website and DNS filtering. Emails are monitored for Virus's, Malware and Spam and are deleted if such issues are found. If these systems cause issues for schoolwork / research purposes, staff should contact the Network Management Company for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature or they feel comes from an untrustworthy source and should immediately report such a communication, to a member of staff.

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people.

Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual, others or bring the school in disrepute.

Pupils must report any accidental access to materials that is deemed inappropriate as per the guidance of this policy directly to the DSL, Headteacher or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the Online-Safety Co-ordinator or Online-Safety Lead for assistance.

The PSHEE curriculum includes advice on what is an appropriate and an inappropriate use of the internet. In addition, the first unit in Computing for Years 1 – 6 focuses on e-safety and the message is re-iterated at all times.

7.0 Data storage and Processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Privacy Policy, Record Keeping Policy and the Acceptable Use Agreements for further details.

Pupils are expected to save all data relating to their work on the school network. Staff are expected to save all data relating to their work to their school laptop/ PC or to the school's central server. All staff hard drives on school devices should only be taken from the building if they are encrypted. Staff should be aware that information stored on the hard drive is not backed up and therefore could be lost in the event of a computer failure.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils data should be stored on external storage devices , but instead stored on the encrypted laptop provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Network management Company and the School Bursar.

8.0 Password Security

Pupils have storage folders on the server, which are used from Year 1 upwards. Children do not have their own login to the school network.

Staff must not write down their password or share it with others.

9.0 Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are asked not to take videos of their children at school events for their own personal use. The School will take official photographs and record any performances where it is allowed to do so. These will be available to parents. Parents are asked to take photographs of their own children, but if other children are present in the image, to respect everyone's privacy and in some cases protection, these images should not be published anywhere without the permission of the people identifiable in them / the permission of their parents in the case of children, nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers (under the direction of staff) are allowed to take digital / video images to support educational aims on school equipment, but must follow school policies regarding the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

School adheres to the following checklist when publishing images of pupils:

- ensure students are dressed appropriately. At sports events for example, we will not publish pictures of pupils in swimming costumes.
- ensure electronic images are stored confidentially and securely and are accessed only by staff with authority to do so
- never show, copy, or give an image to any unauthorised person
- avoid using the last name of a pupil and will always ensure that parents have consented to use of images before publishing the image

Pupils must not take, use, share, publish or distribute images of others.

School handles the images according to its obligations under the Data Protection Act 2018.

St Peter & St Paul School

10.0 Misuse

St Peter & St Paul School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the Derby and Derbyshire Safeguarding Children Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures in particular the Child Protection and Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in the school in line with our Anti-Bullying Policy and Behaviour, Discipline and Exclusion Policy.

11.0 Complaints

As with all issues of safety at St Peter & St Paul School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL, in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate.

Incidents of or concerns around e-safety must be reported to the school's Designated Safeguarding Lead, in accordance with the school's Child Protection Policy.

Date last reviewed by the Trustee Board: September 2021

A review of this policy, through the Trustee Board and the SLT, is undertaken within 3 years of the last review date.

Signed Head teacher

Signed Chair of Trustees

St Peter & St Paul School

Appendix 1

Pupil Acceptable Use Charter for Prep School Pupils (Years 3 – 6)

St Peter & St Paul School uses lots of different ways of teaching children, including the use of technology such as computers, ipads and the internet. The school makes sure that we can use technology safely. We have learnt that we have to be careful and use the internet safely too. We have learnt that some people don't use technology in a kind way, and we know that it is wrong to use it to be unkind to others. We know that if we don't use the technology and internet properly, our teachers will speak to our parents. We know that if we use technology outside of school in a way that upsets someone in our community or reflects badly on SPSP then the teachers will speak to us and our parents. We have agreed to follow the rules below in our e-safety lessons.

I will keep myself safe by:

- Keeping my passwords secure and not sharing them with others
- Not sharing any personal information about myself when on-line
- Telling an adult if I see anything unpleasant or inappropriate, or anything that makes me feel uncomfortable when I see it online

I will treat others and the school with respect by:

- Looking after all school computers and other equipment.
- Not installing any programs on school computers.
- Not using the internet to cause distress or to bully others.
- Not posting pictures, videos or anything else onto the internet, unless directed by a teacher as part of the lesson.
- Not accessing social networking sites (such as Facebook) during school time.
- Not bringing in mobile phones or other devices that can be connected to the internet.
- Telling an adult if I know someone else isn't using technology in the right way.
- Not putting pressure on others to act in a way which threatens their online safety on the online safety of another pupil
- Not using internet to look at anything that is illegal, inappropriate or abusive.

When using the internet for research I am aware that I:

- Must not use the original work of others and say it is my own work
- Must not download pictures or information if work is protected by copyright
- Must take care to check information is from a reliable and accurate source.

I am aware that the school will check my use of school technology and the internet.

I agree to follow the above rules whenever I use St Peter & St Paul School's technology or my own technology in a way that relates to me being a member of the School.

Signed: _____ (Teacher) Date: _____

Signed by Class _____

St Peter & St Paul School

Appendix 2

Pupil Acceptable Use Charter for Pre-Prep School Pupils (Reception – Year 2)

St Peter & St Paul School uses lots of different ways of teaching children, including the use of technology such as computers, ipads and the internet. The school makes sure that we can use technology safely. We have learnt that we have to be careful and use the internet safely too. We have learnt that some people don't use technology in a kind way, and we know that it is wrong to use it to be unkind to others. We know that if we don't use the technology and internet properly, our teachers will speak to our parents.

We have agreed to follow the rules below in our online-safety lessons.

- I will look after all school computers and other equipment.
- I will follow all instructions when using technology in school.
- I will not use the schools' technology to cause any upset or harm to others.
- I will tell a teacher if I know someone else is not using technology in the right way.
- I will keep my passwords private and will not use other children's passwords.
- I will not use the internet to look at anything that I have not been told to look at by a teacher.

I know that the school will check my use of school technology and the internet.

Signed: _____ (Teacher) Date: _____

Signed by Class _____

St Peter & St Paul School

Appendix 3

Staff Acceptable Use Agreement

I confirm that I have read and understood the online-safety policy and the staff code of conduct and I will use all means of electronic equipment provided by the school and any personal devices which I use for school activity in accordance with this policy and the staff code of conduct.

Terms of Agreement

- I understand that I must use school systems in a responsible way to ensure that there is no risk to my professional or personal online safety or the online safety and security of the systems and other users.

- Any online communications or any communications sent from a school email address will be professional and respectful of others and maintain the reputation of the school.

- To protect my own privacy, I will only use a school email address and school phone numbers (including school mobile phones) as contact details for children and their parents, unless in a case of emergency.

- I will not share any personal telephone numbers, email accounts or social media accounts with pupils.

- I will not communicate with parents using personal phone numbers, email accounts or social media accounts on matters of school business.

- I shall only communicate with parents about matters relevant to School life using official School systems: all such communications will be professional in tone and manner

- To protect the privacy of others I will only store confidential child information, personal child information or data on a device that is encrypted or protected with a strong password. I will ensure that school computers are fully logged off or the screen is locked before being left unattended.

- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

- I will not use my personal mobile phone or other personal electronic equipment to take photographs or videos of children.

- I will only use school equipment to take any photographs or videos of children, with their consent

- I will not use my personal mobile phone or access social media accounts or any website or personal email when with the children.
- I will follow the Staff Code of Conduct in regard to school technology
- Any remote work I do away from the school building will be password protected
- I understand that any personal mobile devices are filtered when used through the school network
- I will treat all equipment belonging to the school with respect and care.
- I understand that the School's digital technology systems are primarily intended for educational use and that I shall only use the systems for personal or recreational use within the rules set out in the School's Staff Code of Conduct and HR Staff Handbook
- I understand that the school may monitor or check my use of school-based ICT equipment and electronic communications.
- I understand that by not following these rules I may be subject to the School's disciplinary procedures.

Name ……

Signed ……

Date ……

St Peter & St Paul School

Appendix 4

Volunteer or Visitor with access to the Network Acceptable Use Agreement

St Peter & St Paul School

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all visitors are aware of their responsibilities when using any form of ICT. All volunteers and visiting professionals who have access to the school network are required to read and sign this agreement and adhere to the following in relation to their conduct.

- I understand that school ICT equipment, including computers, laptops, digital cameras, mobile phones and any other form of communication technology, is provided by the school for the purposes of teaching and learning, and/or ensuring pupils' safety.
- I understand that I am not permitted to use my personal mobile phone or handheld ICT device during working hours while teaching or supervising pupils, unless in exceptional circumstances and approved by the Headteacher.
- I will not install any software or hardware on school ICT equipment without permission.
- I will ensure that all personal data (such as data held on iSAMS) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher.
- I understand that my use of school information systems, including the internet and email, can be monitored and logged and can be made available, on request, to the Headteacher.
- I understand that my own personal digital or mobile cameras are expressly forbidden to be used in school.
- I will respect copyright and intellectual property rights.
- I will comply with the ICT system security and not disclose any passwords provided to my school. I understand that I am responsible for all activity carried out under my username.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead or Head Teacher.

Signed: _____

Print name: _____

Purpose of visit: _____

Date: _____

APPENDIX 5

Use of Mobile Phones and Cameras for EYFS

St Peter & St Paul School EYFS allows staff to bring in personal mobile telephones and devices for their own use.

Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

All staff must ensure that their mobile phones/devices are locked away throughout contact time with children.

Mobile phone calls may only be taken at staff breaks or in staff members' own time. If staff have a personal emergency, they are free to use the school's phone or make a personal call from their mobile either in the Staff Room or in a school office (where no children are present).

If any member of staff has a family emergency or similar and are required to keep their mobile phone to hand, prior permission must be sought from the Head teacher.

Cameras

Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements. It is an effective form of recording their progression in EYFS.

They may also be used on our website and/or by the local press with permission from the parents. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.

Only the Reception cameras and iPads are to be used to take any photos within school or on outings. Images taken on this camera must be deemed suitable without putting the children in any compromising positions that could cause embarrassment or distress.

All staff are responsible for the location of the camera and iPads; these should be put away securely at the end of the day. Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week. Images must only be downloaded by EYFS members of staff.

Under no circumstances must cameras of any kind be taken into the bathrooms. If photographs need to be taken in a bathroom, i.e. photographs of the children washing their hands, then the EYFS Co-coordinator must be asked first and staff be supervised whilst carrying out this kind of activity.

Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

This document should be read in conjunction with the Safeguarding and Child Protection Policy and the Staff Code of Conduct.