Holy Trinity
CE Primary Academy

Great Cheverell
Devizes
SN10 5TL
01380 813 796
www.holy-trinity.co.uk

Online Safety Policy

Vision Statement

At Holy Trinity CE Primary Academy, inspired by and rooted in Christian values and teaching, we nurture children to become aspirational, courageous, compassionate, and joyful young people.

The values of our school: Courage, Joy, Aspiration, and Compassion

Status	**Recommended/Statutory**
Author	**Jeremy Shatford**
Approval Date and by	**November 2021**
Review Frequency	**Annual**
Review Due	**November 2022**
Committee	**FGB**

Contents

1 Introduction

1.1 Holy Trinity CE Primary Academy recognises that internet, mobile and digital technologies provide a good opportunity for children to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success is highly likely to be dependent on their online skills and reputation. We are, therefore, committed to ensuring that all children, staff, and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some children may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

1.2 We are also committed to ensuring that all those who work with children, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2 Responsibilities

2.1 The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety coordinator in this school is Mr D Amor.

2.2 All breaches of this policy must be reported to Mr D Amor.

2.3 All breaches of this policy that may have put a child at risk must also be reported to the headteacher.

2.4 Organisations that are renting or using space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

2.5 If the organisation is operating in school time or when children are on site in the care of the school, then the safeguarding of children is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3 Scope of policy

3.1 The policy applies to:

- children
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

3.2 The school also works with partners and other providers to ensure that children who receive part of their education off site or who are on a school trip or residential are safe online.

3.3 The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online. Parental Online Safety Workshops are offered to parents on an annual basis.

3.4 This policy, supported by its acceptable use agreements (see appendices), is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home learning, and behaviour policy.

4 Policy and procedure

4.1 The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

4.2 The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for children, parents/carers, staff and governors and all other visitors to the school.

5 Use of email

5.1 Staff and governors should use a school email account, including Office 0365, for all official school communication to ensure everyone is protected through the traceability of communication. Staff must not contact children, parents or conduct any school business using a personal email address. Children may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the child's account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for Data Protection. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 and Subject Access Request under the Data Protection Act 2018.

5.2 Staff, governors, and children should not open emails or attachments from suspect sources and should report their receipt to Mrs C Yates the Business Manager and the Data Protection Officer.

5.3 Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e., cyberbullying).

6 Visiting online sites and downloading

6.1 Staff must preview sites, software, and apps before their use in school or before recommending them to children. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer (DPO) with details of the site/service and seek approval from the headteacher. The terms and conditions of the service should be adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

6.2 Any online service that requires user accounts to be created or the sharing of any personal data, staff must have a data protection impact assessment (refer to DPO) completed **before** use.

6.3 Staff must only use pre-approved systems if creating blogs, wikis, or other online content.

6.4 When working with children searching for images should be done through Safe Search or a similar application that provides greater safety than a standard search engine. Though should be taken as no safe search is 100% reliable.

7 Users must not:

7.1 Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals, or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e., images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative).
- Indecent images of vulnerable people over the age of 18 (i.e., images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative).
- Adult material that breaches the Obscene Publications Act in the UK.
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation.
- Promoting hatred against any individual or group from the protected characteristics above.
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy.
- Any material that may bring the school or any individual within it into disrepute e.g., promotion of violence, gambling, libel, and disrespect.
- Reveal or publicise confidential or proprietary information.
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses.
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school.
- Use the school's hardware and Wi-Fi facilities for running a private business.
- Intimidate, threaten, or cause harm to others.
- Access or interfere in any way with other users' accounts.
- Use software or hardware that has been prohibited by the school.

7.2 Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitoring system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

7.3 All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

7.4 The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the headteacher.

8 Storage of Images

8.1 Photographs and videos provide valuable evidence of children’s achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with the data protection act, where they are used only with the written consent of parents/carers which is secured in the first instance on a child’s entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See Data Protection Policy for greater clarification).

8.2 Photographs and images of children are only stored on the school’s agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher, along with the Data Protection Office (DPO). Staff and children may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

8.3 Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

8.4 Staff and other professionals working with children, must only use school equipment to record images of children whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is in the personnel file.

9 Use of personal mobile devices (including phones)

9.1 The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of children.

9.2 In no circumstance does the school allow a member of staff to contact a child or parent/carer using their personal device, see also Code of Conduct.

9.3 Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g., for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child unless there is a pre-specified permission from the Headteacher or Assistant Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

9.4 Children in Year 5 & 6 and lone walkers are allowed to bring mobile phones to school but must not use them during the school day. Phones must be switched off and remain in their school bag. Under no circumstances should children use their mobile phone to take images of:

- Any other child unless they and their parents have given agreement in advance.
- Any member of staff.

9.5 The school is not responsible for the loss, damage, or theft on school premises of any personal mobile device.

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

9.7 Personal mobiles may be used to access school emails and data. It is imperative that the app is only accessible via your web browser and logged out completely after use. Please ensure your device is secured by either a password, pin code or face/touch ID. Never leave your device with the application open. It is the responsibility of the member of staff to ensure their virus protection software is up to date.

10 New technological devices

10.1 New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, children and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher, Assistant Headteacher or School Business Manager before they are brought into school.

11 Reporting incidents, abuse, and inappropriate material

11.1 There may be occasions in school when either a child or an adult receives an offensive, abusive, or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the child or adult must report the incident immediately to the first available member of staff, the headteacher or assistant headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed.

11.2 Holy Trinity CE Primary Academy takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

12 Curriculum

12.1 Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables children to become informed, safe, and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health and Computing Curriculum are central in supporting the delivery of online safety education.

12.2 The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

12.3 It is necessary for children to develop skills of critical awareness, digital resilience, and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Children are taught to recognise the creative, collaborative, cultural, economic, and educational opportunities provided by the internet, mobile and digital technologies.

12.4 Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.
- Learning how to develop a positive online reputation and enhance future opportunities
- e.g., in relationships and employment.
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g., recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e., users may not be who they say they are and may have ulterior motives).
- Understanding the dangers of giving out personal details online (e.g., full name, address, mobile/home phone numbers, school details, password, email address) and the importance of maintaining maximum privacy online.
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.
- Understanding the permanency of all online postings and conversations, including those previously posted on any form of social media.
- Understanding relevant legislation, including copyright, and the importance of respecting other people’s information, reputation, and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse.

13 Staff and Governor Training

13.1 Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is undertaken as annual staff online training.

13.2 New staff are provided with a copy of the online safety policy and must sign the school’s Acceptable Use Agreement as part of their induction and before having contact with children.

13.3 Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendices).

13.4 Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendices).

13.5 Guidance is provided for occasional visitors, volunteers, and parent/carer helpers (Appendices).

14 Working in Partnership with Parents/Carers

14.1 Holy Trinity CE Primary Academy works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the Online Safety Policy effectively and help keep children safe. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

14.2 Parents/carers are asked to read and discuss with each child the Acceptable Use Agreement upon entry to the school. This should be reviewed by the parent/carer on a bi-annual basis. This will take place at the beginning of each Key Stage and halfway through Key Stage 2. A summary of key parent/carer responsibilities will also be provided and is available in the Appendices. The Acceptable Use Agreement explains the school's expectations and child and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

15 Records, monitoring and review

15.1 The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to children and staff are minimised.

15.2 All breaches of this policy must be reported, and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incident recording formats are provided in the Online Safety Folder held in the administration office.

15.3 The school supports children and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

15.4 Governors receive regular summary data on recorded online safety incidents through the headteachers report to governors for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

16 Appendix A -Staff, Governors & Student Teachers Online Safety Acceptable Use Agreement

16.1 Staff, Governors & Student Teachers

16.1.1.1 You must read this agreement in conjunction with the online safety policy and the data protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

16.1.1.2 Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

16.1.2 Internet Access

16.1.2.1 I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the Headteacher and an incident report completed.

16.1.3 Online conduct

16.1.3.1 I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

16.1.3.2 I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

16.1.3.3 I will report any accidental access to or receipt of inappropriate materials or filtering breach to the headteacher.

16.1.3.4 I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

16.1.3.5 I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and/or parents/carers.

16.1.4 Social networking

16.1.4.1 I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or children on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

16.1.4.2 When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers, or children. Privileged information must remain confidential.

16.1.4.3 I will not upload any material about or references to the school or its community on my personal social networks.

16.1.5 Passwords

16.1.5.1 I understand that there is no occasion when a password should be shared with a child or any other person without authority on the school computer.

16.1.6 Data protection

16.1.6.1 I will follow requirements for data protection as outlined in data protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or governing body.
- Personal or sensitive data taken off site must be encrypted.

16.1.7 Images and videos

16.1.7.1 I will only upload images or videos of staff, children or parents/carers onto school approved sites where specific permission has been granted.

16.1.7.2 I will not take images, sound recordings or videos of school events or activities on any personal device.

16.1.8 Use of email

16.1.9 I will use my school email address, Microsoft 365, for all school business. All such correspondence must be kept professional and is open to Subject Access Requests and the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

16.1.10 Use of personal devices

16.1.10.1 I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

16.1.10.2 I will only use approved personal devices in designated areas and never in front of children.

16.1.10.3 I will not access secure school information from personal devices unless a closed, monitoring system has been set up by the school.

16.1.11 Additional hardware/software

16.1.12 I will not install any hardware or software on school equipment without permission of the headteacher.

16.1.13 Promoting online safety

16.1.13.1 I understand that online safety is the responsibility of all staff and governors, and I will always promote positive online safety messages including when setting homework or providing pastoral support.

16.1.13.2 I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, children, or parents/carers) to the headteacher.

16.1.14 Classroom management of internet access

16.1.14.1 I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of children. I will also check the appropriateness of any suggested sites suggested for home learning.

16.1.14.2 If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the headteacher or online safety co-ordinator.

16.1.15 Video Conferencing

16.1.15.1 I will only use the conferencing tools that have been identified and risk assessed by Holy Trinity CE Primary Academy. A school owned device should be used when running video conferences where possible.

16.1.16 User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment and/or my responsibilities as an employee/governor.

Signature ……..……………………..……… Date …………………..
Full Name ………………………….. (printed)
Job title ……………………………………………………………….

17 Appendix B - Peripatetic Teachers/Coaches/ Supply Teachers and Students

17.1 Online Safety Acceptable Use Agreement - Peripatetic Teachers/Coaches/ Supply Teachers and Students

17.1.1.1 This agreement forms part of your professional and safeguarding responsibility in Holy Trinity CE Primary Academy. You must read and sign this agreement. This will be kept on record, and you should retain your own copy for reference.

17.1.1.2 Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

17.1.1.3 The school's online safety policy will provide further detailed information as required.

17.1.2 Internet Access

17.1.2.1 I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

17.1.3 Online conduct

17.1.3.1 I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

17.1.3.2 I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

17.1.3.3 I will report any accidental access to or receipt of inappropriate materials or filtering breach to the headteacher.

17.1.3.4 I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to the headteacher or School Business Manager and others as required.

17.1.3.5 I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and/or parents/carers.

17.1.3.6 Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

17.1.4 Social networking

17.1.4.1 I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or children on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

17.1.4.2 In my professional role in the school, I will never engage in 1-1 exchanges with children or parent/carers on personal social network sites.

17.1.4.3 My private account postings will never undermine or disparage the school, its staff, governors, parents/carers, or children. Privileged information known because of my work in the school must remain confidential.

17.1.4.4 I will not upload any material about or references to the school or its community on my personal social networks.

17.1.5 Passwords

17.1.5.1 I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a child or anyone else who is not authorised.

17.1.6 Data protection

17.1.6.1 I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs, and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding the data protection act 2018.

17.1.6.2 Images and videos

17.1.6.3 I will only upload images or videos of staff, children or parents/carers onto school approved sites where specific permission has been granted or other lawful purpose has been identified.

17.1.6.4 I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, child's or parent/carer devices can be used, with parent/carer agreement.

17.1.6.5 Internet, mobile and digital technologies provide helpful recording functions, but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement or other lawful purpose, on a school device, an organisational device approved by the headteacher, or a young person's or parent/carer's own device.

17.1.7 Use of Email

17.1.7.1 I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

17.1.8 Use of personal devices

17.1.8.1 I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me because of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

17.1.8.2 I will only use approved personal devices in designated areas and never in front of children. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support child learning. Children can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

17.1.9 Additional hardware/software

17.1.9.1 I will not install any hardware or software on school equipment without permission of the headteacher.

17.1.9.2 Promoting online safety

17.1.9.3 I understand that online safety is part of my responsibility, and I will always promote positive online safety messages, including when setting homework, rehearsal, or skill practice or when providing pastoral support.

17.1.9.4 I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, children, or parents/carers) which I believe may be inappropriate or concerning in any way to the headteacher.

17.1.10 Classroom management of internet access

17.1.10.1 I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of children.

17.1.10.2 If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the headteacher or online safety co-ordinator.

17.1.11 Video Conferencing

17.1.11.1 I will only use the conferencing tools that have been identified and risk assessed by Holy Trinity CE Primary Academy. A school-owned device should be used when running conferences, where possible.

17.1.12 User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation’s contract with the school.

Signature …………………………………………… Date ……………………
Full Name ………………………………………………………………………………… (Please use block capitals)
Job Title/Role ……………………………………………………………………

18 Appendix C - Visitors, Volunteers, and Parent/Carer Helpers

18.1 Requirements for visitors, volunteers, and parent/carer helpers (Working directly with children or otherwise).

18.2 This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

18.3 Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to children and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSP or headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about children, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free surf the internet in front of children. If I am in any doubt about the appropriateness of the content, I plan to use I will check with my contact in the school.

18.4 Social networking

18.5 I understand where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

18.6 In my school role, I will never engage in 1-1 exchanges with children or parent/carers on personal social network sites.

18.7 My private account postings will never undermine or disparage the school, its staff, governors, parents/carers, or children. Privileged information known because of my work in the school must remain confidential.

18.8 I will not upload any material about or references to the school or its community on my personal social networks.

18.9 User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation’s contract with the school.

Signature …….………………………………..… Date ……………………

Full Name ……………………………….. (Please use block capitals)

Job Title/Role …………………………….…………………….……………

19 Appendix D - cyberbullying incidents

19.1 Guidance on the process for responding to cyberbullying incidents.

19.1.1 All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community most cases can be dealt with through mediation and/or disciplinary processes.

19.1.2 The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported to the online safety co-ordinator immediately. Children should report to a member of staff (e.g., class teacher, headteacher) and staff members should seek support from a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform the headteacher so that the circumstances can be recorded.
- The headteacher will designate a member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- The headteacher will arrange for a member of staff will investigate.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking are also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.