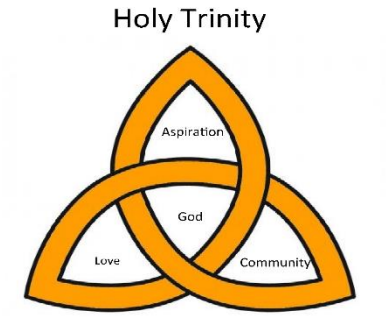
Online/E-Safety Policy

Vision

Our vision is that children are nurtured to love learning, love one another and love God.

'Love learning, love one another, love God.'

Love the Lord your God with all your heart, soul, mind and strength and love your neighbour as yourself (Mark 12)



Policy written by	Jordyn Campbell & Anna Lane
Governors' Responsible	PPCC
Status	Statutory
Review Cycle	Annual
Date written/last review	To be approved by FGB Spring 1 2021
Date of next review	Autumn 2022

Contents

1. Introduction and Overview

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Holy Trinity CE Primary School with respect to the use of ICT-based technologies
- Safeguard and protect the pupils and staff of Holy Trinity CE Primary School
- Assist school staff working with pupils to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced and malicious allegations made against adults who work with students

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (including exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content
- Extreme radicalisation websites

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including hacking Facebook profiles and sharing passwords)

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online including on the internet or gaming
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.2 Scope

This policy applies to all members of Holy Trinity School community (including staff, pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Holy Trinity School.

1.3 Related Legal Documents

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online/E-safety behaviour that takes place out of school.

The 2019 Teaching Online Safety in School gives guidance to school leaders, staff and governing bodies about the importance of teaching pupils how to navigate the online world safely and confidently. It emphasises that having a understanding of the risks that exist online is important to teach children effectively, especially with consideration for vulnerable pupils. This document also refers to Education for a Connected World (2020).

1.4 Related School Policies and Documents

The safeguarding and child protection policy emphasises the welfare of our pupils is paramount. It has a section on Online Safety which includes reference to 'Youth Produced Sexual Imagery' (sexting). It outlines that although technologies and the internet are a source of entertainment, that some adults and young people can use it to harm children. Staff, pupils and parents are encouraged to consider measures to keep themselves and the pupils safe.

The behaviour policy aims to encourage pupils to take responsibility and manage their behaviour to ensure pupils grow in a safe and secure environment. It highlights the expectation that every member of the school community will behave in a considerate way towards others which includes online. Within the behaviour policy, the anti-bullying policy is outlined. It states that everybody has the right to be treated with respect with a specific reference to online bullying (cyber-bullying).

The code of conduct outlines inappropriate behaviour that could lead to a reasonable person to question your conduct, intentions or suitability to work with other people's children. This specifically prohibits using IT to contact and communicate with pupils in an improper manner.

The remote learning policy highlights the importance of consistency in the approach to remote learning for all pupils (including SEND) who are not in school through use of quality online and offline resources and teaching videos. It provides clear expectations for members of the school community with regards to delivery of high quality interactive remote learning.

1.5 Communicating the Online/E-Safety Policy

Communication will occur in many ways but mainly in the following:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school
- Acceptable Use Agreements to be held in personnel files

2. Roles and Responsibilities

This section outlines the key responsibilities regarding Online/E-Safety and the person responsible (see the Monitoring section for further responsibilities):

2.1 Head Teacher

- To take overall responsibility for Online Safety provision
- To take overall responsibility for data and data security (SIRO)
- To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant
- To be aware of procedures to be followed in the event of a serious Online Safety incident
- To ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures (e.g. network manager)

2.2 Designated Safeguarding Lead

- Takes day-to-day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online/E-Safety policies/documents
- Promotes an awareness and commitment to online safeguarding throughout the school community.
- Ensures that Online/E-Safety education is embedded across the curriculum
- Liaises with school ICT technical staff
- Communicates regularly with SLT and the designated Online Safety Governor/committee to discuss current issues and review incident logs
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- Ensure that an Online/E-Safety incident log is kept up to date
- Facilitates training and advice for all staff
- Liaises with the Local Authority and relevant agencies
- Keeps updated in Online/E-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate on-line contact with adults/strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media

2.3 Online/E-Safety Governor

- Ensure that the school follows all current Online Safety advice to keep pupils and staff safe
- Approve the Online Safety Policy and review the effectiveness of the policy
    - This will be carried out by the Governors receiving regular information about Online/E-Safety incidents and monitoring reports
- Support the school in encouraging parents and the wider community to become engaged in Online Safety activities
- Regular review with the Designated Safeguarding Lead (including reviewing Online/E-Safety incident logs)

2.4 Computing Curriculum Leader

- Oversee the delivery of the Online Safety element of the Computing curriculum
- Liaise with the Designated Safeguarding Lead regularly
    - Including ensuring that the curriculum is meeting the needs of the pupils
- To assist teachers with Online/E-Safety lesson planning

2.5 Network Manager

- Report any Online Safety related issues that arise to the DSL
- Ensure that users may only access the school's network through an authorised and properly enforced password protection policy, in which passwords are frequently changed
- Ensure that provision exists for misuse detection and malicious attacks e.g. keeping virus protection up to date
- Ensure the security of the school Computing system
- Ensure that access controls/encryption exist to protect personal and sensitive information eld on school-owned devices
- Ensure the school's policy on web filtering is applied and updated on a regular basis
- Keep up to date with the school's Online Safety policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- Ensure the use of the network/Google Drive/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/DSL for investigation
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keep up-to-date documentation of the school's e-security and technical procedures

2.6 Data Manager

- Ensure that all data held on pupils on the school office computers have appropriate access controls in place

2.7 Teachers

- Embed Online/E-Safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities if relevant)
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

2.8 All Staff

- Read, understand and help promote the school's Online/E-Safety policies and guidance
- Read, understand, sign and adhere to the school Staff Acceptable Use Agreement (see appendices)
- Be aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices and monitor their use and implement current school policies regarding these devices
- Report any suspected misuse or problem to the Online Safety coordinator
- Maintain an awareness of current Online Safety issues and guidance e.g. through CPD
- Model safe, responsible and professional behaviours in their own use of technology
- Ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. personal email, text, mobile phones etc.

2.9 Pupils

- Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (see appendices)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (KS2)
- Understand the importance of reporting abuse, misuse or access to inappropriate materials

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Know and understand school policy on the use of mobile phones, digital cameras and handheld devices (KS2)
- Know and understand school policy on the use of images and on cyber-bullying.
- Understand the importance of adopting good Online/E-Safety practice when using digital technologies out of school and realise that the school's Online/E-Safety Policy covers their actions out of school, if related to their membership of the school
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home

2.10 Parents/Carers

- Support the school in promoting Online/E-Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images (see appendices)
- Read, understand and promote the school Pupil Acceptable Use Agreement with their children
- Access the school website and Google Classroom/Meet in accordance with the relevant school Acceptable Use Agreement
- Consult with the school if they have any concerns about their children's use of technology

2.11 External Groups

- Any external individual/organisation will sign an Acceptable Use Agreement prior to using any equipment or the internet within school (see appendices)

3. Monitoring

It is the responsibility of each member of staff to adhere to the policy, standards and procedures and to report any breach of the policy immediately to DSL. Members of staff should also record and report any online aspect to any safeguarding, behaviour or safety-related incident. This includes extremist or discriminatory behaviour.

The Computing Subject Leader (Anna Lane) has responsibility for supporting staff in maintaining the Online/E-Safety policy in teaching and learning and in communicating online/e-safety messages to pupils and to the wider school community.

The DSL (Alison Bateman) has direct responsibility for maintaining the policy, standards and procedures and providing advice on their implementation.

The Network Manager (Andrew Turner) has direct responsibility for ensuring the protection and integrity of school information.

Governors will monitor online safety as part of their safeguarding responsibilities. This falls within the terms and conditions of the Pupils, Parents & Community Committee.

The DSL has overall responsibility for the policy particularly with regards to:

- Regular review
- Ensuring that where any safeguarding, behaviour or safety-related incident involves online aspects, that these aspects are recorded and responded to appropriately
- Responding to any extremist or discriminatory behaviour shown by pupils.
    - This may lead to the school involving other agencies including the Local Authority Designated Officer, social services or police as appropriate. It may also lead to the school invoking Safeguarding procedures if appropriate

4. Communication with Stakeholders

This policy must be shared with all members of the school community.

4.1 Staff

- Annual training on online/e-safety for all staff is required, together with formal induction for new staff which will often be included within safeguarding training
- Staff are given the Staff Handbook, Code of Conduct to read and refer to when joining the school
- Staff are asked to complete the Staff AUP annually (see appendices) *

4.2 Pupils

- Teaching and learning about online/e-safety is embedded in the curriculum, both in discrete lessons as part of the Computing subject curriculum and in general teaching when opportunities arise
- Pupils are taught that general school expectations on behaviour extend to online life
- Pupils are asked to complete the Pupil AUP annually (see appendices) *

4.3 Club Providers

- Provisions of this policy are to be shared with Club Providers through the website and are asked to read it if working with online resources in school

4.4 Supply Teachers

- Provisions of this policy are to be shared with Club Providers through the website and are asked to read it if working with online resources in school

4.5 Visitors

- Provisions of this policy are to be shared with Club Providers through the website and are asked to read it if working with online resources in school

4.6 Parents, Carers, Governors and Others

- Provisions of this policy are to be shared with parents, carers, governors and others through the school website
- The PTA and other affiliated organisations are to be requested to abide by this E-Safety Policy
- Parent/Carers are asked to complete the Parent AUP annually (see appendices) *
- Governors are asked to complete the Governor AUP annually (see appendices) **

*The staff, pupil and parent/carers AUPs are stored either physically (pupil) or electronically (staff, parents) by the Computing coordinator.

**The governors AUPs are stored by the Clerk to the governors

5. Data security

5.1 Purpose

The purpose of this part of the E-Safety Policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of Holy Trinity Primary School to ensure that:

- Information will be protected against unauthorised access

- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Online/E-Safety training will be available to all staff

It is the responsibility of the DSL to establish what information needs to be secured, how the information changes over time, who else can use it and why.

All breaches of ICT security, actual or suspected, must be reported to, and will be investigated by the DSL.

5.2 GDPR

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place. The law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.

6. Acceptable Use

6.1 Summary of Key Responsibilities of Staff

- To look after the equipment that they are using
- To act responsibly with any data or files they are using
- To report any broken or malfunctioning equipment to the Computing Subject Leader and Network Manager as soon as possible
- To report any lost or stolen equipment to the Computing Subject Leader and Network Manager
- To report any loss of data to the Network Manager
- To respect the privacy of others and the reputation of the school
- To remain vigilant for any breaches of school ICT security and contact the appropriate member of staff if issues are uncovered

6.2 School Infrastructure

- All school infrastructure is to be secured with hardware and software solutions to avoid unauthorised access and inappropriate use
- All computers, including PCs, laptops, iPads and other devices, are to be secured with suitable hardware and software security for safe and appropriate use by adults and pupils
- The use of all technology in the school is governed by the Acceptable Use provisions of this Policy (in addition, any equipment provided by the school for use outside the school should be used in accordance with these rules)
- Technology that can be used to store, transmit or manipulate data, including photos, such as media-rich phones, cameras, MP3 players and laptops, should be used responsibly and in accordance with the Acceptable Use provisions of this Policy, particularly when taken off-site
- Network and system security are in place for everyone's protection. Members of staff must respect this and always follow the Data Security Policy
- Members of staff must not download or install software to school computers. Only the Network Manager may do this
- Staff must be aware of the threats posed by viruses and malicious code and should take steps to avoid infection of any technology; this includes ensuring that they have anti-virus software installed on home

computers (the use of USB memory sticks or portable devices is not encouraged; however, if they are used then they must be encrypted and scanned for viruses on school devices before they are opened)
- Members of staff are responsible for material downloaded, created, stored or transmitted by them. It is the staff's responsibility to ensure that it does not cause offence or anxiety to others or break the law
- Members of staff should not attempt to repair equipment themselves
- Any loss of data should be reported immediately to the Network Manager

6.3 Account Security

- Members of staff are responsible for the protection of their own account details and should not divulge passwords to anyone
- Passwords should be a combination of letters, numbers and special characters and should use both lowercase and capital letters. They should avoid easily guessable words, such as class names or usernames
- Passwords should not be written down, saved in web browsers if offered to do so, or emailed to anyone
- Members of staff (excluding the DSL) should not log on to or use any account, other than their own, and should log off or lock workstations when leaving them, even for just a short period of time (the DSL has the right to logon to any school email account)
- When members of staff have finished using computers, they should log off, to allow others to log in

6.4 Internet Access

- Staff should ensure that they are not breaking copyright restrictions when using material from the internet
- Members of staff should only visit appropriate children sites
    - The school will periodically monitor and record (log) the websites that members of staff visit
- Members of staff are not permitted to access public chat facilities, instant messaging, social networking, blogging websites at school
- If members of staff access public chat facilities, instant messaging, social networking, blogging and wikis websites at home, they should ensure that they:
    - Do not use school provided equipment to do so
    - Act responsibly, preserving and safeguarding the confidential information that they are privy to at school
    - Respect the privacy of others and the reputation of the school
    - Do not breach the school's Security Policy
    - Do not use a screen name that is offensive or gives away additional personal information
    - Do not supply personal or contact information relating to the school, about themselves or others via the Internet

6.5 Email

- When using email to communicate safeguarding, behaviour or safety concerns, staff must follow guidance from the SEN department in the use of technology to record and/or communicate confidential information concerning children using CPOMs
- Staff should not open emails or attachments from senders that they do not recognise, or that look suspicious (e.g. executable files containing the filename extension .exe)
- Staff should be wary of links to websites in emails, especially if the email is unsolicited
- Staff should not send sensitive information by email unless it is encrypted
- If a member of staff receives an email which is offensive or upsetting, then the DSL (or Deputy DSL in their absence) should be contacted (the email in question should not be deleted until the matter has been investigated)
- Staff are responsible for all emails they send
- Staff should distribute their email address responsibly and not supply personal or contact information about themselves or others via email
- Staff should report any spam or phishing emails that are not blocked or filtered to the Network Manager

- Staff should use the school's contacts or address book (this helps to stop emails being sent to the wrong address)
- Staff should not try to bypass the school's security measures to access email off-site (for example, forwarding email to a personal account)
- Staff should not reply to, add to, or circulate chain emails

6.6 Laptops and Other Devices

- Staff should lock/sign out of their laptops when leaving them unattended.
- Staff should shut down their laptops using the 'Shut Down' or 'Turn Off' option and not use hibernate or standby.
- Staff should try to prevent people from watching them enter passwords or view sensitive information.
- Staff should store laptops and other devices securely.
- Staff should not leave their laptops and other devices unattended unless they trust the physical security in place.
- Laptops and other devices should not be left in a car; however, if this is unavoidable, they should be temporarily locked out of sight or in the boot
- Unauthorised people should not be allowed to use staff laptops/desktops and other devices.
- Refer to the Remote Learning Policy for more information

6.7 Use of still and moving images

Staff sign the school's Acceptable Use Agreement which includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils. Staff should take care when using photographs or video footage of pupils on the school website and other places to reduce the risk of inappropriate, unsolicited attention from people outside the school:

- Consider using group photographs rather than photos of individual children
- Do not use the first name and last name of individuals in a photograph
- If showcasing school-made digital video work, take care to ensure that pupils are not referred to by name on the video, and that pupils' full names are not given in credits at the end of the film
- If showcasing examples of pupils' work consider using only their first names, rather than their full names
- Only use images of pupils in suitable dress to reduce the risk of inappropriate use

An easy rule to remember is:

> If the pupil is named, avoid using their photograph / video footage.
> If the photograph / video is used, avoid naming the pupil.

6.8 School Website

The Deputy-Headteacher (Lucy Ashby) takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained:

- The school website complies with the school's guidelines for publications
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the website is the school address and telephone number (teacher's work email addresses are also available)
- Photographs published on the web do not have full names attached
- Parental/carer permission is gained for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website

6.9 Safe Use of Technology by Pupils

6.9.1 Teaching and Learning: Requirement

Pupils are, as part of the Computing Subject in the National Curriculum, taught to:

- find information on the internet
- publish on the Internet
- collaborate online and to use a variety of computer programmes, apps and online services

The school acts in various ways to ensure the maximum possible safety:

- Using network level filtering
- Ensuring search engines and sites such as YouTube are set by default to SAFE
- Teachers use their professional judgement to direct children to appropriate internet websites and services
- The school uses age-appropriate apps on iPads and other tablets (where possible, the school uses tablet apps without embedded adverts or advertising)

6.9.2 Teaching and Learning: Online/E-Safety

Pupils in KS1 and KS2 are taught online/e-safety in Computing lessons; and whenever technology is included in other lessons or broader discussion. This teaching includes:

- Class discussion and agreement to age-appropriate Pupil Acceptable Use Agreements
- Following the school's Online/E-Safety curriculum (see appendices)
- Online working, including collaboration, email and social media must be prefaced with preparatory online/e-safety teaching
- Use of online tools often requires the creation and use of online identities/accounts which must be prefaced with preparatory online/e-safety teaching, preventing the use of real names and other identifiable information

6.9.3 Trips and Other Settings

Where pupils go on trips or attend other settings, staff should ensure that venues, if they provide online access, do so with appropriate Online/E-Safety Policy (this should be recorded in the risk assessment)

6.10 Mobile Phones

Use by staff of personal mobile phones and other personal devices to support teaching and learning is discouraged. Where staff do choose to use their own mobile phones and other devices, care and professional judgment should be paramount. Staff should consider the provisions of this policy, especially in avoiding the retention and sharing of still and moving images of pupils, and in never recording full names of children or any other information which can make a child identifiable.

6.11 Support

Staff who have any concerns about a pupil regarding safeguarding, behaviour or safety with any online aspect must immediately speak to a senior leader.

If you have any questions, comments or requests with regards to the systems in place, please do not hesitate to contact the Computing Subject Leader or the DSL.

Faulty equipment should be reported to the Computing Subject Leader or the Network Manager.

6.12 Handling of Complaints/Infringements

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible

to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available for deliberate misuse include:

- Use of stage 2 or 3 as described in the School Behaviour Policy
- Interview/counselling by Class Teacher and/or DSL
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to the Local Authority/Police

Any complaint about staff misuse is referred to the Head Teacher (or Deputy DSL if absence or involved).

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

7. Appendices

Staff Code of Conduct

Holy Trinity CE Primary School

Safeguarding children and young people
Code of Conduct

At Holy Trinity School we expect staff to act as positive role models and set good examples at all times to our pupils. Holy Trinity School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. The following is, therefore, a code of conduct for all adults working in or on behalf of the school, including those involved in home visits or any out of school activities.

You should always:

- Behave in a mature, respectful, safe, fair and considered manner at all times.
- Observe other people's right to confidentiality (unless you need to report something to the Head Teacher or senior designated teacher e.g. concerns about a child protection issue).
- Treat all children equally; never favour one particular child, or build 'special relationships' with individual children, except where one to one working is part of a plan agreed with your manager.

Report to the Head Teacher (or in the case of an allegation concerning the Head Teacher, the Chair of Governors) as soon as possible:

- Any behaviour or situation which may give rise to complaint, misunderstanding or misinterpretation against yourself.
- Any difficulties that you are experiencing, for example, coping with a child presenting particularly challenging behaviour; situations where you anticipate that you may not be sufficiently qualified, trained or experienced to deal with or handle appropriately.
- Any behaviour of another adult in the school which give you cause for concern re breach of this code of conduct or other school policies and procedures.

You should never:

- **Behave in a manner that could lead a reasonable person to question your conduct, intentions or suitability to work with other people's children.**
- Touch children in a manner which is or may be considered sexual, threatening, gratuitous, secretive, intimidating or may represent a misuse of authority.
  (It is not possible to be specific about the appropriateness of each physical contact for key adults on the staff team, since an action that is appropriate with one child in one set of circumstances may be inappropriate in another, or with a different child. You should therefore, use your professional judgement at all times.)
- Discriminate either favourably or unfavourably towards any child.
- Give personal contact details, text, email or telephone except for agreed work purposes using work IT, or make arrangements to contact, communicate or meet children outside of work.
- Develop 'personal' or sexual relationships with children.
- Push, hit, kick, punch, slap, throw missiles at or smack a child or threaten to do so.
- Be sarcastic, embarrass or humiliate, make remarks or "jokes" to children of a personal, racist, discriminatory, intimidating or otherwise inappropriate* or offensive nature.
- Give or receive (other than 'token') gifts unless arranged through your line manager / Head Teacher, for example, outgrown sports kit, football boots or uniform.
- Allow, encourage or condone children to act in an illegal, improper of unsafe manner e.g. smoking or drinking alcohol.

- Behave in an illegal or unsafe manner, for example, speeding, being under the influence of drugs or alcohol, driving a vehicle which is known to be un-roadworthy or otherwise unsafe, or not have appropriate insurance, use a mobile phone whilst driving, fail to use seatbelts or drive in an unsafe manner whilst transporting children.
- Undertake any work with children when you are not in a fit and proper physical or emotional state to do so.

***Please note:**
It is the perception of the person subject to a remark or action rather than your stated intention that defines 'appropriate' or 'inappropriate'.

These expectations apply to all contact with our pupils including activities out of school such as baby sitting and tutoring.

If you have any concerns about a child or the conduct of an adult please ensure that you contact the Designated Officer as soon as possible. These are the people to contact:
Mrs Alison Bateman – Head teacher – designated officer
Miss Lucy Ashby – Deputy head – deputy designated officer
Mrs Fiona Whiteside – Inclusion manager
You can also speak to any members of the Senior Leadership Team.

If your concern is about the Head teacher then please contact the Chair of governors, Mrs Michele Marcus (mmarcus@htprimary.com) or the Vice Chair of governors, Revd Dan Wells (dwells@htprimary.com) or the governor who is responsible for safeguarding, Francis Neal (fneal@htprimary.com)
You can also contact the Local Authority Designated Officer on 0208831 6008 or 07774332675
The local Single Point of Access is 020 8547 5008

7.1 Online/E-Safety School Curriculum

Year 1 Autumn Term	E-safety (Autumn 1): • Teach e-safety rules: https://www.thinkuknow.co.uk/4_7/hectorsworld/ (one video per lesson with discussion)

Year 2 Autumn Term	E-safety (Autumn 1): • Review e-safety rules: https://www.thinkuknow.co.uk/4_7/6-7-year-olds/ • Talk about the differences between real and online experiences. • Introduce sharing information online; emails, communicating and navigating safely. • Keeping personal information safe. • Importance of talking to a trusted adult about their online experiences.

Year 3 Autumn Term	E-safety (Autumn 1): • Review e-safety rules: https://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew (one video per lesson with discussion) • Check knowledge by completing quizzes

Year 4 Autumn Term	E-safety (Autumn 1): • Review e-safety rules: http://www.thinkuknow.co.uk/8_10/ • Create a resource to help young children remember the e-safety rules e.g. poster, chatterbox, video etc.

Year 5 Autumn Term	E-safety (Autumn 1): • Review e-safety rules: chatting with care, using text and picture messaging, behaving responsibly • Use the Internet (children's search engines) to research their work and recognise the need to ask appropriate questions to find appropriate answers • Practice interpreting information from online research, rather than copying • carry out more refined web searches by using key words • Identify the validity of a website by discussing inaccurate or biased sources • Develop strategies to ignore or cancel unsolicited advertising (pop-ups, banners, videos or audio • Acknowledge sources used in their work

Year 6 Autumn Term	E-safety (Autumn 1): • Review e-safety rules • Hamilton Trust resources: https://www.hamilton-trust.org.uk/topics/upper-key-stage-2-topics/e-safety-mini-topic/e-safety-and-digital-citizenship/ • Use a range of sources to check the validity of a website. • Recognise that different viewpoints can be found on the web and critically evaluate the information they use, and understand some of the potential dangers of not doing so

	• Discuss the issues of plagiarism, copyright and data protection in relation to their work • Discuss copyright free images and sounds from sources such as the Audio Networks and NEN image gallery

7.2 Acceptable Use Agreement: Staff (and visitors)

Holy Trinity CE Primary School

Acceptable Use Agreement: Staff

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should always be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse.

Professional integrity and strong moral purpose must always be upheld by staff. It is the duty of all staff members to ensure that children in their care get the best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

The school's internet, network and ICT systems and subscriptions to services should always be used with the utmost professionalism. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.

 I will never upload images/video imagery of staff/pupils to my personal social media accounts.

- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviours/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.

- I know what GDPR is and how this has a bearing on how I access, share, store and create data.

- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.

- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.

- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity whilst using it.

- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.

- I shall keep all usernames and passwords safe and never share them.

- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely.

- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.

- Any data collected on a mobile phone/camera will be used in accordance with school policies both in school and on school trips/outings.

- When using personal devices for capturing images/ video, I will upload them to the school systems and remove them as soon as possible from my personal device.

- When using personal devices for contacting parents, I will block my number using the code '141'.

7.3 Acceptable Use Agreement: Governors

Acceptable Internet and E-Safety use conduct for Governors

Introduction

This Acceptable Use Agreement covers use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or school umbrella body (Local Authority).

This document also covers school equipment when used outside of school, use of online systems provided by the school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Holy Trinity regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

Acceptable internet and E-Safety Use

- The Head Teacher/IT coordinator should be notified immediately if users receive questionable material or chance upon an undesirable website
- Emails sent to an external organisation should be written carefully and checked before sending in the same way as a letter written on school headed paper. Avoid the autofill of contacts facility and check recipients before sending to ensure information remains secure.
- Encrypt or Pin protect any document containing sensitive information before sending it to any recipient. Agree the PIN code via another communication method – phone, text as appropriate.
- Keep personal details safe and do not give them out over the internet.
- Everyone should develop and maintain knowledge of internet safety issues, particularly with regard to how they might affect children
- Only the schools approved Internet Service Provider (ISP) should be used for internet use
- Change school passwords regularly to a “strong” password which includes capitals, lower case, numbers and symbols and should contain at least 8 characters. Change password immediately if it is compromised
- Ensure that the password auto save function is turned off.

Unacceptable use of the internet

- It is not acceptable to access, transmit or create any offensive, obscene or indecent images, sounds, data or other material, as well as material that is defamatory, violent, supporting extremist views, abusive, racist, homophobic or that may cause needless anxiety
- Do not bring the name of the school into disrepute
- Breach of confidentiality that results in information being inappropriately made available to others, including through social networking sites used from phones and home computers
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018
- Transmission of commercial or advertising material or access to gambling websites
- Violate the Data Protection Act 2018 by deliberately corrupting or destroying other users’ data or violating the privacy of others

- Disrupting the work of others or wasting the time of staff or other users
- Do not download any software or resources from the internet that can compromise the network or bypass filtering and security systems or are not adequately licensed

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head Teacher will use their professional judgement to determine whether any act or behaviour not

on the list above is considered unacceptable use of the school's IT facilities.

Access to school IT facilities and materials

The school's IT coordinator and IT Provider manage access to the school's IT facilities and materials for school staff and governors. That includes, but is not limited to:

- Computers, tablets and other mobile devices
- Access permissions for certain programmes or files
- Use of copier facilities

Personal use of IT facilities including copying must not be overused or abused.

Authorised users will be provided with unique log-in/account information and passwords that they must use when accessing the school's IT facilities, these must not be shared or borrowed. One user, One login.

All documents, data etc. which are printed, saved, accessed and delete/shredded in accordance with the school's network and data security protocols.

Governors who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT coordinator/IT provider.

Use of email

- The school provides each Governor with an email address. This email account should be used for school purposes only. Unless with the specific agreement of the FO or Head Teacher
- Governors should use the agreed Governor Hub for sharing documents and information in relation to their role as governors
- Any information downloaded from Governor Hub onto a personal device should be deleted upon the completion of the task
- All school-related business should be conducted using the email address the school has provided
- Governors must not share their personal email addresses with parents and pupils and must not send any governor-related materials using their personal email account
- Users must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract
- Email messages are required to be disclosed in legal proceedings or in response to Subject Access requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, therefore do not write anything you would not want read by others
- Governors must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals should be encrypted so that the information is only accessible by the intended recipient

- If Users receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information
- If staff send an email in error which contains the personal information of another person, they must inform the FO immediately and follow our data breach procedure

Use of Phones

- Governors must not give their personal phone numbers to parents or pupils
- School phones must not be used for personal matters
- Governors who are provided with the use of a mobile phone as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4
- If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so
- No images or videos should be taken on mobile phones or personally owned devices. It is not permitted to take photos or videos of children on personal devices. Where photos are taken at staff social events, these should not be published without the express agreement of the people involved
- Governors are not permitted to use their own mobile phones for contacting children or their families within or outside of the school in a professional capacity
- Governors should never send to, or accept from anyone, texts or images that could be viewed as inappropriate or allow children to be 'friends' on social networking sites
- All users with school emails should ensure their phones are protected with PIN codes in case of loss or theft
- Governors can give the school office number as an emergency contact number for dependents during the working day to minimise the need for checking mobile phones

Social Media

Governors should take care to follow the school's guidelines on social media use.

Monitoring of school network and use of IT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised IT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises

- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

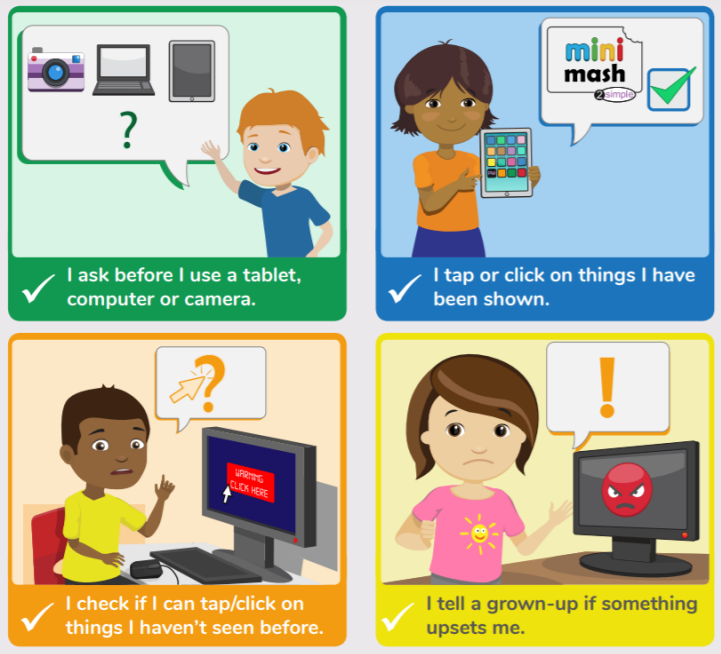
Please sign below to say that you have read and understood this information and have read and will follow the Holy Trinity's School Online Safety Policy (including mobile and hand held devices). This is on the school website.

7.4 Acceptable Use Policy: Early Years Pupils

Holy Trinity CE Primary School

Acceptable Use Policy

Early Years



7.5 Acceptable Use Policy: KS1 Pupils

Holy Trinity CE Primary School

Acceptable Use Policy

Key Stage 1

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post to Google Classroom, use our email and other communication tools.

7.6 Acceptable Use Policy: KS2 Pupils

Holy Trinity CE Primary School

Acceptable Use Policy

Key Stage 2

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access Google Classroom and subscription services.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something is not working correctly or is damaged.
- I will use all communication tools such as Google Classroom, email and blogs carefully.
- I will notify an adult immediately if I notice that someone who is not approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.

T = is it true?
H = is it helpful?
I = is it inspiring?
N = is it necessary?
K = is it kind?

- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed, and appropriate actions taken.

7.7 Acceptable Use Policy: Parents/Carers

Holy Trinity CE Primary School

Acceptable Use Policy

Parents/Carers

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe regarding online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are always responsible users of digital technologies.

Acceptable Use Agreement

We would ask parents and carers to support us by:

- Sharing good online behaviours with your child.
- Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- Explaining how to keep an appropriate digital footprint.
- Discussing what is and is not appropriate to share online.
- Emphasising never to meet anyone online nor trust that everyone has good intentions.
- Reporting any concerns you have whether home or school based.
- Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.