HOLY TRINITY C of E SCHOOL, East Finchley

High Standards Together

'At Holy Trinity School we promise to provide opportunities for every child to be the best that they can be.

We aim to create a happy and secure Christian environment in which children can grow in confidence and independence.

We strive for excellence in teaching and learning to achieve high standards together.'

Online Safety Policy

Date: October 2020

Sub Committee to review	FSB
Target Audience	All staff, Governors
Curriculum / non curricular	Non curricular
Associated Policies / Documents	Safeguarding, Anti-Bullying
New Policy or Review of existing policy.	Review
Date of Submission	November 2020
Date for Review	November 2021
Reviewed	Annually
Date ratified by Governors	

Statement of intent

At **Holy Trinity CE School**, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- **Human Rights Act 1998**
- **Data Protection Act 1998**
- **Freedom of Information Act 2000**
- **Regulation of Investigatory Powers Act 2000**
- **Safeguarding Vulnerable Groups Act 2006**
- **Education and Inspections Act 2006**
- **Computer Misuse Act 1990, amended by the Police and Justice Act 2006**
- **Communications Act 2003**
- **Protection of Children Act 1978**
- **Protection from Harassment Act 1997**

1.1. This policy also has regard to the following statutory guidance:
DfE (2020) 'Keeping children safe in education'

1.2. This policy will be used in conjunction with the following school policies and procedures:

- **Safeguarding Policy**
- **Behaviour Policy**
- **Whistle blowing Policy**
- **Acceptable Use Policy**
- **Sex Education Policy**
- **Complaints Policy**
- **Image use Policy**
- **Staff code of conduct**
- **Anti-bullying Policy**
- **Data Protection Policy**

2. Use of the internet

- The school understands that using the internet is important when raising educational standards, promoting pupil achievement, and enhancing teaching and learning.
- Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

- When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:
    - Access to illegal, harmful or inappropriate images
    - Cyber bullying
    - Access to, or loss of, personal information
    - Access to unsuitable online videos or games
    - Loss of personal images
    - Inappropriate communication with others
    - Illegal downloading of files
    - Exposure to explicit or harmful content, e.g. involving radicalisation
    - Plagiarism and copyright infringement
    - Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

- It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.
- The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
- The **Computing Lead**, **Stacey Man**, is responsible for ensuring the day-to-day online safety in the school and managing any issues that may arise.
- The Computing lead is responsible for monitoring of curriculum across the school.
- The **Computing Lead** is responsible for communicating to and with representatives of the school **senior leadership team (SLT)**, teaching staff, governors, parents, pupils and wider school community regarding online safety
- The **headteacher** is responsible for ensuring that the **Computing Lead** and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.
- The **Computing Lead** will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.
- The **headteacher** will ensure there is a system in place which monitors and supports the **Computing Lead**, whose role is to carry out the monitoring of online safety in the school, keeping in mind data protection requirements.
- The **Computing Lead** will regularly monitor the provision of online safety in the school and will provide feedback to the **headteacher**.
- The **Computing Lead** will review a log of submitted online safety reports and incidents on a termly basis.
- The **headteacher** will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- The **Computing Lead** and **Safeguarding Lead** will ensure that all members of staff are aware of the procedure when reporting online safety incidents, and will keep a log of all incidents recorded.
- The **Computing Lead** will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs

the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

- Cyber bullying incidents will be reported in accordance with the school's Behaviour **Anti-Bullying Policy**.
- The governing body will monitor the effectiveness of the online safety provision, current issues, and to review incident logs, as part of the school's duty of care. Which may include holding meetings with the **Computing Lead**.
- The **governing body** will evaluate and review this Online safety Policy on a **termly** basis, taking into account the latest developments in ICT and the feedback from staff/pupils.
- The **headteacher** will review and amend this policy with the **Computing Lead**, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- Teachers are responsible for ensuring that online safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- All staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online safety Policy.
- All staff and pupils will ensure they understand and adhere to our **Acceptable Use Policy or Home Agreement**, which they must sign and return to the **headteacher**.
- Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
- The **headteacher** is responsible for communicating with parents regularly and updating them on current online safety issues and control measures.
- All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.
- This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.
- This policy applies to any online activity with any form of device/computer produced or sent at any time which affects any other student(s) staff or the wider community and or brings the school in to disrepute. School sanctions and the behaviour policy applies.
- Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.
- Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.
- The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

4. Online safety education

Educating pupils:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold online safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety. Online safety group will be facilitated by the **Computing Lead and the Online Safety Lead.**

Educating staff:

- A programme of online safety training opportunities is available to all staff members, including whole school activities and CPD training courses.
- All staff will undergo online safety training on a **termly** basis to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the internet as a whole.
- All staff will undergo regular audits by the **Computing Lead** in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this Online safety Policy.
- The **Online Safety Lead** will act as the first point of contact for staff requiring online safety advice.

Educating parents:

Holy Trinity recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We will build a partnership approach to online safety with parents and carers by ensuring that:
- Online safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and letters.
- Twilight courses and presentations which will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any online safety related concerns.
- It is the responsibility of parents and carers to:
- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and/or acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Online safety control measures

Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in line with our **Acceptable Use Policy**.
- A record will be kept by the **headteacher** of all pupils who have been granted internet access.
- All users will be given usernames and passwords for different sites used in school, and are advised to keep these confidential to avoid any other pupils using their login details.
- Pupils activities are continuously monitored by the **Computing Lead**.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the **headteacher**.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the **Computing Lead** for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices.

Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Pupils at this school may use the LondonMail / PupilMail system from LGfL for all school emails.
- Staff at this school use the StaffMail system for all school emails.
- Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, the chat functionality of Google Classroom, homework submission tool and Class Dojo are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the Headteacher (the particular circumstances of the incident will determine whose remit this is) should be informed immediately. Google Classroom chat is different to Gmail, and Education Gmail manged by the school is not the same as a private Gmail account
- The use of personal email accounts to send and receive personal data or information is prohibited. No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
- Internally, staff should use the school network, including when working from home when remote access is available via Freedom 2 Roam and G Suite.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the Education Gmail system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are **not** monitored.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

6. Cloud platforms:

- Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.
- This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.
- As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our DP policy.
- For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud.
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought where necessary.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Two-factor authentication is used for access to staff or pupil data.
- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used by students or staff to store pupil work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

7. Social networking

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the **headteacher**.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the **headteacher** prior to accessing the social media site.

Social Media

- Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.
- This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
- Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.
- However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.
- Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.
- Email/Parentmail is the official electronic communication channel between parents and the school, and between staff and pupils.
- Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.
- Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.
- Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the school).
- ** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

- All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

8. Published content on the school website and images

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value.

- The **headteacher** will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

9. Mobile devices and hand-held computers

- The **headteacher** may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils.
- Staff can use their personal mobile devices in designated mobile phone zones. See appendix 1.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the **Computing Lead** when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

10. Network security

- Network profiles for pupil's and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords should be stored using non-reversible encryption.

Virus management

- Technical security features, such as virus software, are kept up-to-date and managed by the Computing Lead, who may delegate to the relevant technician.
- The Computing Lead will ensure that the filtering of websites and downloads is up-to-date and monitored.

11. Online Safety.

Online safety committee

- The Online safety Policy will be monitored and evaluated.
- This will include a member of the SLT, the Computing Lead and the designated safeguarding Lead (DSL), as well as members of the governing body.

Cyber bullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Holy Trinity.
- For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.
- The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Behaviour Policy.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Holy Trinity and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. (Settings will need to highlight specifically how internet use will be monitored either here or within previous sections)
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Reporting misuse

- Holy Trinity CE School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

- Inappropriate activities are discussed and the reasoning behind prohibiting activities due to online safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use that takes place at any time and affects, student(s) staff, or the wider community
- Any instances of misuse should be immediately reported to a member of staff, who will then log this on My Concern.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the concerns and parents may be asked to attend a meeting with a Designated Safeguarding lead.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff

- Any misuse of the internet by a member of staff at any time should be immediately reported to the headteacher, following the Complaints Policy.
- The headteacher will deal with such incidents in accordance with the Whistleblowing Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Use of illegal material

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL/Deputy Lead will be informed and the police contacted.

Monitoring and review

- The online safety committee will evaluate and review this Online safety Policy on a termly basis, taking into account the latest developments in ICT and the feedback from staff/pupils.
- This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.
- Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
- Full information can be found in our information security policy.

12. Management of Applications (apps) used to Record Children's Progress

- We use Tapestry, Google Classroom, Class Dojo and Educater to track learners progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

13. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2020.
- Holy Trinity recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding and Anti-bullying policy.
- Holy Trinity recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Holy Trinity also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Holy Trinity will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. (Identify resources or policies as appropriate)
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

- If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy. (Amend as appropriate)
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- Holy Trinity recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Holy Trinity will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. (Identify resources as appropriate)
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.

- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Holy Trinity will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Holy Trinity recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. (Include where this can be accessed, e.g. website, intranet, etc.)

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or the Police.

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Holy Trinity will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Education Safeguarding Service.

If made aware of IIOC, we will:
- Act in accordance with our child protection policy and the relevant Safeguarding Child Boards procedure
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF) and the police.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:
- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
- Ensure that the headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Appendix 1

Acceptable Use of Mobile Phones & Camera Policy

- It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Mobile Phones

- Holy Trinity School allows staff to bring in personal mobile telephones for their own use. However
- all staff must ensure that their mobile telephones are left inside their locker provided throughout contact time with children and during their working day.
- Users bringing personal mobile telephones into Holy Trinity C.E Primary school must ensure there is no inappropriate or illegal content on the device.
- Mobile phone calls may only be taken during staff breaks or in staff members' own time. If staff have a personal emergency they are free to use the school office phone or make a personal call from their mobile in the designated mobile phone zones.

These mobile phone zones can currently be found in:

- Staffroom
- Deputy Headteacher/SENCO office
- Headteacher Office
- Family Liasion Officer's Office.
- After school Club Kitchen.
- Main school office
- If a member of staff is waiting for an emergency personal call please speak to the headteacher.
- Staff will need to ensure that the Office has up to date contact information and that staff make their families, children's schools etc, aware of emergency work telephone numbers. This is the responsibility of the individual staff member.
- All parent helpers will be subject to this policy and will be asked to take or receive any calls in the designated mobile phone zones.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Head Teacher or Deputy Head Teacher.
- Concerns will be taken seriously, logged and investigated appropriately in line with our safe guarding policy.

Visitors /Workmen

- Mobile phones are only to be used in the designated mobile phone zones. In addition to the staff mobile phone zones, visitors are also free to use their mobiles in the front office area. If it is necessary for visitors/workmen to have their mobile phones to implement their role effectively then they are to be supervised at all times. Members of staff are expected to challenge visitors if they have concerns and will always inform the headteacher of any breaches our policy.

Cameras

- Photographs are only to be taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements and are an effective form for recording their progression in the Early Years Foundation Stage. Photographs may be taken of children in all year groups for use within school and only with prior consent of their parents. They may also be used on our website and/or by the local press with permission from the parents.
- However, it is essential that photographs are taken and stored appropriately to safeguarding

- Only the designated Holy Trinity C.E Primary School mobile devices i.e. iPad or cameras are to be used to take any photos within the setting or on outings.
- Only Holy Trinity C.E Primary School devices to be used to play music or images for events and assemblies
- Images taken on these mobile devices or cameras must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the location of the devices. Images taken and stored on the devices must be downloaded on site as soon as possible and deleted from the storage media on the mobile device used to take the pictures.
- Under no circumstances must mobile devices or cameras of any kind be taken into the children's toilet area without prior consultation with the Head Teacher or Deputy Head Teacher.
- If photographs need to be taken in the toilet area i.e. photographs of the children washing their hands, then the Headteacher or Deputy Head Teacher must be asked first and staff to be supervised whilst carrying out this kind of activity. At all times the mobile devices or cameras must be placed in a prominent place where it can be seen.
- Photographs maybe taken during productions/outings if permission has been granted by the Headteacher or Deputy Head Teacher as occasionally there are restrictions for safety reasons. If permission is granted then photographs are only for parent/carers personal use and must not be placed on any social network sites.
- Failure to adhere to the contents of this policy will lead to disciplinary action being followed in line with Safeguarding procedures.