Online Safety Policy
2022-23

Our Mission Statement

Holy Trinity and S. Silas
Our Mission Statement

Holy Trinity and S. Silas School was founded by the Church in 1847 to serve the community and to provide an education for every child in the area.

We offer all our children an education of the highest quality taught through the arts and lived through the principles and practice of the Christian faith. We provide a place where all children and adults know their contribution is valued and where they can develop their own faith in God and in one another.

We aim to help every child develop to their full potential, to achieve highly, succeed, and grow in confidence and abilities. Our inspiring curriculum provides all the skills every child will need for life, it develops their self-confidence, awakens their imagination and encourages them to think independently.

We value the diversity of backgrounds and cultures which enrich our life and help our school become the unique place it is. The life of our school is integral to that of the Parish: we both contribute to our local community and benefit from it in our achievements.

It is in this way that we prepare our children for the future and fulfil our school motto: 'Fortis in Fide' *('Strong in the Faith')*.

"And let us consider how we may spur one another on toward love and good deeds, but encouraging one another-and all the more as you see the Day of the Lord approaching." (Hebrews 10.25)

Contents

Key contacts

Holy Trinity & S. Silas Primary School

Headteacher:
Name: Lorraine Dolan
Contact details: head@holytrinitynw1.camden.sch.uk

Online safety co-ordinator:
Name: Neil McIntyre and Pam Macmeikan
Contact details: 020 72670771
n.mcintyre@holytrinitynw1@camdne.sch.uk
p.macmeikan@holytrinitynw1.camden.sch.uk

Nominated LGfL contact
Name: Pam Macmeikan / Lorraine Dolan
Contact details: 0207 2670771
p.macmeikan@holytrinitynw1.camden.sch.uk

IT systems manager:
Name: Alex Marinos / – Camden Schools IT Support Services (SITSS)
Contact details: 020 7942465 / 07776245090
Alex.marinos@camden.gov.uk

Designated safeguarding lead:
Name: Lorraine Dolan
Contact details: head@holytrinitynw1.camden.sch.uk

Deputy DSG
Name: Neil McIntyre /Contact: n.mcintyre@holytrinitynw1.camden.sch.uk
Name: Kate Arnison / Contact: k.arnison@holytrinitynw1.camden.sch.uk

Nominated governor:
Name: Jacqui Miller
Contact details: Jacqui.miller7@btinternet.com

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO):
Name: Sonia Forbes
Contact details: 020 7974 4556

Child and Family Contact/MASH team:
Manager: Noella Hacquard
Tel: 020 7974 1553/3317
Fax: 020 7974 3310

Camden online safety officer:
Name: Jenni Spencer
Tel: 020 7974 2866
Prevent Education Officer
Name: Jane Murphy
Tel: 020 7974 1008

1 Online Safety: The issues

1.1 Introduction

The educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. Holy Trinity & S. Silas School needs to be able to teach children how to keep themselves safe whilst on-line.

This policy outlines how this is achieved in school and supports staff to recognise the risks and take action to help children use the internet safely and responsibly.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as online bullying. More details on this can be found in section 4.5 of this policy.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- online bullying (see section 4.5 for further details)
- use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

2 School online safety strategies

2.1 Whole school approach

Computing is now a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Holy Trinity & S. Silas Primary school will consider the following points in order to ensure a holistic approach to online safety:

- Staff will be made aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and should be aware of the use of technology in child-on-child abuse.

- When developing new policies, online safety and the impact of technology will be considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.

- The school will ensure that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff will receive suitable training around online safety and similar messages should be taught to pupils.

- Staff should be aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with pupils, the school will ensure there are clear policies available to staff on expectations for online behaviour.

- There will be a clear link between the online safety policy and the behaviour policy that sets out expected standards for pupil's online behaviour and expected sanctions for breaches.

- School's online safety policies will be reviewed annually and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

Schools should refer to:

DfE non-statutory guidance on teaching online safety:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE:
https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

2.2. Purpose and description

The schools online safety strategy is based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

The purpose of the school's online safety strategy is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet

- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

The school has the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems. The school uses London Grid for Learning platform.

- A culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures that everyone is aware of expected standards of on-line behaviour.

The following polices are in place to support this.

Online Safety Policy
ICT User Agreement – Acceptable Use Policy for Staff & Governors
Email Security & Etiquette Guidance
Safeguarding and Child Protection Policy
Data Protection Policy

Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this is achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

2.3 Roles and responsibilities

The school's online safety strategy is inclusive of the whole school community, including teaching assistants, supervisory assistants, governors and others, and forges links with parents and carers. This policy is approved by governors and overseen by the head teacher and is fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Head teacher's role

The headteacher has ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

2.3.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the head teacher in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors are subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. Governors should, when appropriate, use Governor Hub when conducting school business. Personal emails should not be used for any personal or sensitive information or data relating to staff or pupils.

2.3.3 Online safety co-ordinator's role

The school has two designated online safety coordinators, who are jointly responsible for co-ordinating online safety polices for on behalf of the school. Both co-coordinators are on the Senior Management team and are deputy designated safeguarding leads

Online Safety Coordinators	**Responsibilities**	**Joint responsibilities**
The Deputy Headteacher / Computing Subject leader	**<u>Curriculum and pupils</u>** ensure online safety is embedded in the curriculum provide the first point of contact and advice for school staff, governors, pupils and parents report annually to the board of governors on the implementation of the school's online safety strategy	develop, implement, monitor and review the school's online safety policy ensure that staff and pupils are aware that any online safety incident should be reported to them

The School Business Manager	**<u>Computing network, related systems and external agencies</u>** assess the impact and risk of emerging technology and the school's response to this in association with SITSS IT staff and learning platform providers raise the profile of online safety awareness within the school by ensuring access to training and relevant online safety literature ensure that all staff and pupils have read and signed the acceptable use policy (AUP) maintain a log of internet related incidents and co-ordinate any investigation into breaches report all incidents and issues to Camden's online safety officer.	liaise with the school's Camden SITSS, the Head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems Provide support or advice to all staff, governors' pupils and parents where required or requested

The online safety co-ordinator receives recognised training to carry out their role more effectively, i.e. CEOP or E-PICT

2.3.4 Camden Schools IT Support Service (SITSS)

Their role is:

- To manage all devices, ensuring connection via the wireless router is secure including HTS-CURRICULUM, filter for pupils.
- Centrally manage the downloading of software
- To provide guest login numbers for added security
- To white / black any individual websites as requested by the online safety coordinators
- To respond to network issues / server problems and secure backups
- Liaise with the online safety coordinators on issue arising, trend and security alerts, changes
- Provide a fully managed security service that includes, antivirus & malware protection and internet filtering systems.

2.3.5 Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's online safety and acceptable use policy and procedures
- communicating the school's online safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the online safety co-ordinator
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator
- teaching the online safety and digital literacy elements of the new curriculum.

2.3.6 Designated safeguarding leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead/s who will decide whether or not a referral should be made to Children's Safeguarding and Social Work or the Police.

2.4 Pupils with special educational needs and disabilities (SEND)

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. The school will have a flexible and personalised approach to online safeguarding for those pupils in order to meet their needs.

SEND co-ordinators are responsible for providing extra support for these pupils and should:

- link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND
- where necessary, liaise with the online safety co-ordinator and Camden SITSS to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND
- ensure that the school's online safety policy is adapted to suit the needs of pupils with SEND
- be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences
- liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.

2.5 Working with parents and carers

The Online Safety Policy and Computing Policy are available for parent/carers to download from the school website. Parents / carers sign an acceptable use agreement (see Appendix 2) on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Most children will have internet access at home or on their own mobile devices. Parents are able to contact the school's online safety coordinators if they have any concerns about their child's use of technology.

The school offers annual online safety training opportunities for parents in order to provide them with information to help them keep their child safe online. The CSCB online safety leaflet for parents is available on the CSCP website: https://cscp.org.uk/parents-and-carers/online-safety/. The school also publishes this on the school website and will provide a link to the information at a minimum annually in the school newsletter.

When teachers are teaching their class about online safety and any related issues, they make parents aware of and reinforce online safety messages that should be reinforced at home.

Where remote online learning is being used, parents will be made aware of what arrangements have been made, which websites children will be accessing and which members of staff they will be interacting with online.

3 Online safety policies

3.1 Accessing and monitoring the system

- Access to the school internet system are via individual log-ins and passwords for staff and pupils have a class login. Visitors are given permission from the headteacher or online safety co-ordinator to access the system and are given a separate visitors log-in.

- Staff are required to change their password to access the network every six months

- The online safety co-ordinator and teaching staff should carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

3.2 Confidentiality and data protection

- The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.

- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system. The school currently uses Egress Switch, LGFL My Drive, School2school and CPOMs. Any breaches of data security should be reported to the head teacher immediately.

- CCTV, notices is displayed in a prominent place to ensure staff and pupils are aware of this, and recordings will not be revealed without appropriate permission.

3.3 Acceptable use policies

- All internet users within the school will be expected to sign an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use

- Acceptable use agreements for pupils will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet in school (see appendix 2).

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 3).

The school Business manager will keep a copy of all signed acceptable use agreements in the Staff files.

3.4 Teaching online safety

3.4.1 Responsibility

When developing the teaching of online safety, the school will have regard to the Department of Education guidance *teaching online safety in schools* available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

One of the key features of the school's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the Computing subject leader, but all staff should play a role in delivering online safety messages.

- The online safety co-ordinator who is also the computing subject leader is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.

- The online safety co-ordinator who is also the Computing Subject Lead is to liaise with teaching staff on planning and delivering online safety lesson.

- The online safety co-ordinator should ensure that any external resources used for teaching online safety have been thoroughly reviewed in advance

- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.

- The School is required to teach about online bullying as part of statutory Relationships Education (primary), Relationships and Sex Education (secondary) and health education (all schools)

- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers may wish to use PSHE lessons *and during statutory relationships and sex education* as a forum for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- The school will teach online safety in a safe environment that allows pupils to discuss issues in an open, honest and non-judgemental way and it is recommended that the designated safeguarding lead is involved in the development of any lessons teaching online safety

- As these discussions may lead to pupils recognising that they have been harmed online, teachers should be aware that following discussions, pupils may wish to make a disclosure

- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.

3.4.2 Content

Pupils will be taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies;

- can evaluate and apply information technology, including new or unfamiliar technologies;
- are responsible, competent, confident and creative users of information and communication technology.

Pupils are taught all elements of online safety included in the computing curriculum and Statutory Relationships Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help
- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.
- how to recognise techniques used to persuade or manipulate, for example extremist views, grooming and targeted marketing
- what is and is not acceptable online behaviour
- identifying online risks
- how to get help and support.

Statutory Health Education teaching will include:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted

- where and how to report concerns and get support with issues online.

3.5 Staff training and conduct

3.5.1 Training

- All school staff and governors receive policies and procedures with regard to IT systems and online safety as part of their induction and where required can meet with the online safety co-ordinators.

- Staff also receive specific training on online safety so that they are aware of the risks and actions to take to keep pupils safe online. School management should ensure that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

3.5.2 IT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.

- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images taken on allocated school ipads should be erased.

- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff should be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.

- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with parents regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.

- When making contact with parents by email, staff should always use their school email address or account. Personal email addresses and accounts such as Facebook should never be used.

- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops or i-pads provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5.3 Exit strategy

When staff leave, the school business manager is responsible for ensuing that any school equipment is handed over and that PIN numbers, passwords and other access codes are reset and the staff member is removed from the school's IT system.

3.6 Safe use of technology

3.6.1 Internet and search engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.

- Pupils should be supervised at all times when using the internet.

- Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.

- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet

resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety co-ordinator/s who will liaise with the IT service provider for temporary access. Teachers should notify the online safety co-ordinator once access is no longer needed to ensure the site is blocked.

3.6.2 Evaluating and using internet content

Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

School email systems is hosted by LGFL which allows content to be filtered. The children at HTSS do not hold a school email account and the use of personal email is not permissible

Social networking sites such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has access to the site. These are not used in school but pupils may well use these sites at home.

Online communities and forums are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

Chat rooms are internet sites where users can join in “conversations” on-line; **instant messaging** allows instant communications between two people on-line. In most cases, pupils will use these at home although school internet systems do host these applications.

Gaming-based sites allow children to “chat” to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites are not be accessible via school internet systems

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- If the school identifies a clear educational use for emails or social networking sites and forums for on-line publishing, the sites must be approved by the

online safety coordinator. Any use of these sites should be strictly supervised by the responsible teacher.

- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety co-ordinator who will liaise with the learning platform provider.

- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.

- Pupils are taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

- Pupils are taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.

- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils are warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.

- Users are aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

In order to teach pupils to stay safe online outside of school, they are advised:

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

- to only use moderated chat rooms that require registration and are specifically for their age group;

- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them

- how to set up security and privacy settings on sites or use a “buddy list” to block unwanted communications or deny access to those unknown to them

- to behave responsibly whilst on-line and keep communications polite

- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else

- not to arrange to meet anyone whom they have only met on-line or go “off-line” with anyone they meet in a chat room

- to behave responsibly whilst on-line and keep communications polite

- to behave responsibly whilst on-line and keep communications polite

- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.6.4 Video conferencing and remote learning

Video conferencing and live streaming enables users to communicate face-to-face via the internet using web cameras.

The school has a remote learning / working user agreement in addition to the ICT acceptable use policy. The following London Grid for Learning guidance is taken into account:

https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- *only using school registered accounts rather than personal accounts*
- *recording remote learning for safeguarding purposes*
- *the security of the video link*
- *checking settings regularly to ensure teachers have full control of the meeting ie; who can start, join or chat in the stream*
- *paying attention to background settings to prevent breach of privacy*
- *training for teachers to use the new technology*
- *a system for teachers to log any remote learning contacts and issues.*

3.6.5 School website

- Class teachers and specialist teachers have responsibility for uploading their class/subject page with appropriate information and photographs. The Senior Administration Officer and senior management have responsibility for uploading all other material and information. Staff with access to the website is all class teachers, Head Teacher and Deputy Head Teacher, School Business Manager & Senior Administrative Officer.

- The online safety co-ordinators and the head teacher / deputy head teacher are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- To ensure the privacy and security of staff and pupils, the contact details on the website is the school address, email and telephone number. No contact details for staff or pupils are contained on the website.

- Children's full names are never published on the website.

- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.6.6 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.

- Written permission is obtained from parent/carers, when their child starts school, to allow photographs/videos of their children on the school website.

- Children's names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

- Staff should not use personal devices to take photographs of pupils.

- The school does not permit parents to take photographic images of school events, such as performances and assemblies.

3.6.7 Pupils and staff own mobile devices

Children are not allowed to bring mobile devices to school with the exception of Year 6 children. They are allowed to bring mobile phones into school but they must be turned off and left at the school office.

All staff must not use their mobile telephones in their classrooms areas or in the playground. They should only be used in the staff room or off site. Mobile phones must be switched off in the classroom or whilst on playground duty, lunchtime duty and during meetings. The school is not responsible for the loss or damage of mobile telephones.

Where staff access the school internet system via their own devices, the same acceptable use agreements apply and sanctions may be applied where there is a breach of school policy.

4 Responding to incidents

4.1 Policy statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety co-ordinator in the first instance. All incidents, whether involving pupils or staff, must be recorded by the online safety co-ordinator on the online safety incident report form (appendix 4).

- A copy of the incident record should be emailed to Camden's designated online safety officer at jenni.spencer@camden.gov.uk.

- Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action under staff conduct policies for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors. Managing Allegations Against Staff and Volunteers & LADO - Camden Safeguarding Children Partnership — CSCP

- The school's online safety co-ordinator/s should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.

- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated safeguarding lead, who will make a decision as to whether or not to refer the matter to the police and/or Children's Safeguarding and Social Work in conjunction with the head teacher.

Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the online safety co-ordinator/s and details of the website address and URL provided.

- The online safety co-ordinator should liaise with the Camden SITSS or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

4.3 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

- The incident should be reported to the online safety co-ordinator and details of the website address and URL recorded.

- The online safety co-ordinator/s should liaise with the IT system manager or learning platform provider to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the online safety co-ordinator immediately. If the misconduct involves the head teacher or governor, the matter should be reported to the chair of the board of governors.

- The online safety co-ordinator will ensure the computer, laptop or other device is taken out of use and securely stored in order to preserve any

evidence. A note of any action taken should be recorded on the online safety incident report form.

- The online safety co-ordinator will arrange with the IT SITSS or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the head teacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.

- If the materials viewed are illegal in nature the head teacher or governor should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.

4.5 Online bullying

4.5.1 Definition and description

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, sexting/"happy slapping").

Online bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school. All incidents will be dealt with under the schools Behaviour Policy and child-on-child abuse guidance. Schools

and Nurseries Safeguarding Policies - Camden Safeguarding Children Partnership — CSCP

- The school's behaviour and anti-bullying policy and acceptable use policies cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of online bullying should be reported to the online safety co-ordinator/s who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.

Pupils are taught:

- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to send or post inappropriate images of themselves
- not to respond to offensive messages
- to report the matter to their parents and teacher immediately.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The pupil should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The pupil should also consider changing email address.

- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Online bullying of school staff

- Head teachers should be aware that school staff may become victims of online bullying by pupils and/or their parents. Because of the duty of care owed to staff, head teachers should ensure that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents.

- The issue of online bullying of school staff should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.

- Incidents of online bullying involving school staff should be recorded and monitored by the online safety co-ordinator in the same manner as incidents involving pupils.

- Staff should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.

- Personal contact details for staff should not be posted on the school website or in any other school publication.

- Staff should follow the advice above on online bullying of pupils and not reply to messages but report the incident to the head teacher immediately.

- Where the bullying is being carried out by parents the head teacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.

4.6 Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute sexual harassment or online bullying and because of the nature of online activities, this can lead to more widespread harm and repeat victimisation.

Keeping children safe in education places a duty on schools to respond to any incidents of online sexual harassment such as:

- consensual and non-consensual sharing of nude and semi-nude images
- sharing explicit and unwanted content and images
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats
- coercing others into sharing images or performing acts online that they are not comfortable with.

The School is aware of the duty under statutory guidance *Keeping children safe in education* and *Sexual violence and sexual harassment between children in schools and colleges* which requires schools to have policies in place to deal with incidents of online sexual harassment. Schools will refer to the *child-on-child Abuse and Sexual Violence guidance for schools and colleges* for further details on what actions need to be taken in response to online sexual harassment. Schools and Nurseries Safeguarding Policies - Camden Safeguarding Children Partnership — CSCP

The schools will make pupils aware that producing and distributing sexual images to peers via the internet or mobile devices may be illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

The school will remain vigilant and aware of when any of these behaviours may be linked to the sexual exploitation of a pupil or is being carried out as a gang-related activity. Staff should refer to the CSCP *Extra-familial harm and child exploitation guidance* for further details.
CSCP-extra-familial-harm-and-child-exploitation-guidance.pdf

4.7 Risk from inappropriate contacts with adults

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of pupils being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the online safety co-ordinator/s and the designated safeguarding lead.

- The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Children's Safeguarding and Social Work and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The designated safeguarding lead can seek advice on possible courses of action from Camden's online safety officer in Children's Safeguarding and Social Work.

- Teachers will advise the pupil on how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated safeguarding lead and the online safety co-ordinator should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school IT equipment or networks, the online safety co-ordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.8 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised

as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

Holy Trinity & S. Silas School (HTSS) have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- Pupils and staff know of the risks of becoming involved in groups with extremist ideologies and the tactics they may use to groom and exploit. Staff and young people should also be made aware that accessing and sharing certain content is against school policies and certain contact with certain groups is illegal.

- All school staff who use the internet as part of their lessons need to be aware of their responsibilities to promote good conduct, support young people to be aware of the dangers of contact and how to put security in place and how to recognise and report inappropriate content. This is part of building young people resilience which is one of the 6 strands of the Prevent Duty

- HTSS ensures that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism. School Leaders and Class Teachers agree how the internet is accessed in school and which staff are available to support children in the usage. Also children should be able to support one another to filter content and report concerns they have for each other

- All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.

- The online safety co-ordinator/s and the designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.

- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer to MASH. If there is imminent danger dial 999. In all other circumstances follow the schools

safeguarding procedures by speaking to the DSL. If next steps are not clear speak to the Prevent Education Manager or refer directly to MASHadmin@camden.gov.uk

Schools may contact the Prevent Education Manager for advice on any of the above

Further information is available in the CSCB guidance "Safeguarding children and young people from radicalisation and extremism" available at: https://cscp.org.uk/resources/radicalisation-and-extremism-resources/

4.9 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.

- Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor

- Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

5 Sanctions for misuse of school IT

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

School policy -referral to the online safety co-ordinator and/or headteacher -contact parent/carers

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

School policy -referral to the headteacher with possibility of suspension -removal of mobile phone -contact parent/carers

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- online bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

School policy -referral to the headteacher with possibility of suspension or exclusion -removal of mobile phone -contact parent/carers

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme online bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

School policy

-referral to the headteacher with possibility of suspension or exclusion
-removal of mobile phone
-contact parent/carers
-referral to community police officer or police
-referral to Camden's online safety office

5.2 Sanctions for staff

These reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the school code of conduct.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher *as a low level incident in line with the school's staff conduct policy.*

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable un encrypted memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

School policy
-referral to the head teacher who will issue a warning

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO under the CSCP guidance on dealing with allegations against staff and volunteers. Managing Allegations Against Staff and Volunteers & LADO - Camden Safeguarding Children Partnership — CSCP

.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications

- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

School policy
-referral to the headteacher -removal of equipment -referral to Camden's online safety officer -referral to Camden's LADO or the police -suspension pending investigation -disciplinary action in line with school policies

Policy Reviewed December 2022

Policy approved by governors: Resources Committee 19 January 2023
Next review date: January 2024

Links with other Policies

Pupils Acceptable Use Policy – Appendix 2
ICT User Agreement - Acceptable use policy for staff and governors – Appendix 3
Home/ remote working agreement

Appendix 1:

Online safety incident report form
This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

School/organisation's details:

Name of school/organisation:

Address:

Name of online safety co-ordinator:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (online bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
□ terrorist material
□ online grooming
□ online radicalisation
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ online bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to head teacher/senior manager
□ advice sought from LADO
□ referral made to LADO
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to head teacher/senior manager
□ advice sought from Children's Safeguarding and Social Work
□ referral made to Children's Safeguarding and Social Work
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken

□ child/young person debriefed
□ online safety policy to be reviewed/amended

Outcome of incident/investigation

Appendix 2

Holy Trinity & S. Silas Primary School

Pupils Acceptable Use Policy

Pupils Name:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- *keep my password a secret*
- *only open pages which my teacher has said are okay*
- *not look at or delete other people's files*
- *talk to my teacher before using anything on the internet*
- *not use internet chatrooms*
- *ask for permission before opening an email or an email attachment*
- *not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)*
- *not load any photographs of myself onto the computer*
- *never agree to meet a stranger*
- *make sure all the messages I send are polite and sensible*
- *tell my teacher if anything makes me feel scared or uncomfortable or I receive a nasty message*
- *not reply to any nasty message which makes me feel upset or uncomfortable*
- *not give my mobile number, home number or address to anyone who is not my real friend*
- *only email people if my teacher agrees*
- *only use a school email address for agreed work such as through Purple Mash*
- *not bring in any digital files to school without permission*

I know

- *that the school may check my computer files and monitor the internet sites I visit*
- *if I deliberately break the rules, I could be stopped form using the Internet or computer*

Parents

- *I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.* □

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of email and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Pupils Name:

Year Group:

Parent/ Caretaker:

Signed:

Date:

Appendix 3

Holy Trinity & S. Silas Primary School

ICT User Agreement
Acceptable use policy for staff and governors

Outline

This ICT user agreement covers the 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 Local Authority, or other information or systems processors.

This ICT user agreement also covers school issued equipment (as logged on the asset register) when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.

This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.

The school regularly reviews and updates with the assistance of the DPO, all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.

User Requirements

- All computer networks and systems belong to the school and are made available to staff and governors for educational, professional, administrative and governance purposes only.

- Staff and governors are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or governors being removed
.
- The school reserves the right to monitor internet activity and examine and delete files from the school's system.

- Staff and governors have a responsibility to safeguard pupils in their use of the internet and reporting all online safety concerns to the online safety coordinators

- Copyright and intellectual property rights in relation to materials used from the internet must be respected.

- E-mails and other written communications must be carefully written and polite in tone and nature.

- Anonymous messages and the forwarding of chain letters are not permitted.

- Staff and governors will have access to the internet as agreed by the school but will take care not to allow pupils to use their logon to search the internet.

- Only schools approved email system(s) for any school business are permissible for staff
- Staff and governors will follow good practice advice at all times and will ensure online activity meets the standards expected of professional conduct.

Data protection and system security

- Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems, such as Egress Switch, USO- FX2 through LGFL or Governors Hub. Where personal data is taken off the school premises via laptops, memory sticks and other mobile systems, the information must be encrypted beforehand.

- Use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented on the school ICT system using Window Defender Security Centre and Malwarebytes. This is currently on all school Desktops.

- Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.

- Staff and governors are not permitted to download any software or resources from the internet that can compromise the network or might allow staff to bypass the filtering and security system or are not adequately licensed. Advice will be provided from the Online Safety coordinators (Neil McIntyre & Pam Macmeikan) and/or IT systems manager from SSITS (Camden IT services)

- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal and log out of their terminal when they are not at their desk.

- Supply staff are to be given the supply log-in details, this is available in the school office and is written within the supply induction sheets given to the supply teacher on arrival

- Any guest in school requiring access to the network can use the guest log-in this will allow access to programmes on the network but not to any folders. Please ask the office if this is required

- Any guest, which requires access to the internet, will be provide with a separate guest log in access code

- Staff should set strong passwords, following advice provided by the school

- Personal digital cameras or camera phones for taking, editing and transferring images or videos of pupils or staff is not permissible or is the storage of any such images or videos at home or on any personal devices.

- Only school approved equipment for any storage, editing or transfer of digital images / videos will be permissible. Saved photographs and videos of children and staff to be stored on the staff-only drive on the school server. While school ipads can be used to take photographs or videos of staff or children, with the appropriate permissions in place these images must be stored on the secure school server and be deleted from school ipad devices.

- Images published, with parental permission on the school website and other online learning environment etc. will not identify students by name, or other personal

information and must only be uploaded where consent has been obtained by the parent, if you are unclear on consents please check with the school office.

- Remote access to school resources (such as from home) is only permissible using the school approved system and following e-security protocols to interact with them.

- Files should be saved, stored and deleted in line with the school policy.

- Data protection policy requires that any information seen by staff or governors with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data and I will not store any pupil data that is not in line with the school's data policy and adequately protected.

Personal use

- Staff and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal

- Staff and governors should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.

- Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

- School ICT systems may not be used for private purposes without permission from the head teacher.

- Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.

INTERNET USAGE DISCLAIMER

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Camden SITSS has restricted a number of websites (such as social networking, blogs etc). However, neither the school nor Camden LA can accept liability for the material accessed, or any consequences of Internet access.

If an unsuitable site does get through the filtering software then staff and/or pupils are told to give the URL (address) and description of content to the online safety coordinator/s who will inform the SITSS and / or Internet Service Provider.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

User Signature

I have read the above policy and agree to abide by its terms.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date .....

Full Name ..... (printed)

Updated: December 2022

Approved by Resources Committee: 19 January 2023

iPad E-Safety Policy for staff members who have been assigned a school iPad

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc, are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (Which is currently: LGFL Staffmail)
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the school online safety co-ordinator/s.
- I will not download any software or resources from the Internet that could compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other computing 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

* I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

* I agree to abide by all the points above.

* I wish to have an email account; be connected to the Internet; be able to use the school's computing resources and systems.

Signature:

Name:

Date:

IPAD LOAN AGREEMENT FOR STAFF

This document should be completed for each member of staff issued with an iPad

Member of staff Name	
Staff signature	
Member of staff home address	
Member of staff contact phone no.	
Serial number of iPad	
Charger borrowed	
Period of Loan	

Terms

The iPad is the property of the school and it remains so.
It is issued to the member of staff named above for her/his exclusive use during the agreed period.
The member of staff named above must return the iPad at the end of the loan agreement.
The member of staff is expected to take reasonable care of the iPad and to make it available for inspection by the school at any time with reasonable notice. Ensured that it is covered by own contents insurance and must not be left unattended in the boot of a car to and from school.
The member of staff is responsible for ensuring that the iPad is used in accordance with the school e-safety policy. Misuse of the iPad or viewing of explicit material will lead to disciplinary proceedings. If the iPad (or charger if borrowed) is broken or damaged, the member of staff is responsible for repair or replacement and pay any incurring costs.

Authorisation

I agree to the assignment of the iPad to the member of staff named above.

Name:

Signature:

Date: