St Hilary's School
E-Safety Policy

This policy applies equally to the EYFS, Pre-Prep and Prep as taught at St Hilary's School.

Persons responsible for this policy:
Headteacher
IT Manager
Designated Safeguarding Lead

This policy was reviewed in:
November 2023, December 2023

E-SAFETY POLICY

Introduction

At St Hilary's School, we see education as a partnership between the family and the school. Our school is dedicated to preparing our children for their adult life beyond formal education and ensuring that it promotes and reinforces British Values to all our children. We actively promote democracy, the rule of the law, liberty and respect those with different faiths and beliefs. These are fundamental British Values which underpin all that we offer, as does our School Motto 'Not for oneself but for all.'

1. AIMS

St. Hilary's aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and Governors;
- identify and support groups of pupils that are potentially at greater risk of harm online than others;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology; and
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- **Contact** — being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharingof nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head Masters and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. ROLES AND RESPONSIBILITIES

3.1. The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Body will also make sure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (**DSL**).

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the School has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Governing Body will review the DfE filtering and monitoring standards, and will discuss with IT staff what needs to be done to support the School in meeting those standards, which include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- reviewing filtering and monitoring provisions at least annually;
- blocking harmful and inappropriate content without unreasonably impacting teaching andlearning; and
- having effective monitoring strategies in place that meet their safeguarding needs.

The Governor who oversees online safety is Simon Allen in his role of the Safeguarding Governor.

All Governors will:

- ensure they have read and understand this policy;
- agree and adhere to the terms on acceptable use of the School's ICT systems and the internet (Appendix 4);

- ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures; and

- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (**SEND**). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2. The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the School.

3.3. The Designated Safeguarding Lead

Details of the School's DSL are set out in the School's Safeguarding (Child Protection) Policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the School, in particular:

- supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the School;

- working with the Headteacher and Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;

- taking the lead on understanding the filtering and monitoring systems and processes in place on School devices and the School network;

- working with the IT Manager and the Network Manager to make sure the appropriate systems and processes are in place;

- working with the Head teacher, IT Manager and other staff, as necessary, to address any online safety issues or incidents;

- managing all online safety issues and incidents in line with the School's Safeguarding (Child Protection) Policy;

- ensuring that any online safety incidents are logged (see Appendix 6) and dealt with appropriately in line with this policy;

- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School's Behaviour, Rewards and Sanctions Policy;

- updating and delivering staff training on online safety;

- liaising with other agencies and/or external services if necessary;

- providing regular reports on online safety in school to the Headteacher and/or Governing Body;
- undertaking annual risk assessments that consider and reflect the risks children face; and
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4. The IT Manager and the Head of Digital Learning

The IT Manager and the Head of Digital Learning are responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist andextremist material;
- ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- conducting a full security check and monitoring the School's ICT systems on a regular basis;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- ensuring that any online safety incidents are logged (see Appendix 6) including Filtering and Monitoring (Appendix 7) and dealt with appropriately in line with this policy; and
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School's Behaviour, Rewards and Sanctions Policy.

This list is not intended to be exhaustive.

3.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy;
- implementing this policy consistently;
- agreeing and adhering to the terms on acceptable use of the School's ICT systems and the internet (Appendix 4), and ensuring that pupils follow the School's terms on acceptable use (Appendices 1 and 2) and the pupil iPad contract (Appendix 3);

- knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing. Staff are asked to email their concerns to the DSL;
- working with the DSL to ensure that any online safety incidents are logged (see Appendix 6) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School's Behaviour, Rewards and Sanctions Policy; and
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Staff will complete the self-audit set out in Appendix 5 at least annually.

3.6. Parents/carers

Parents/carers are expected to:

- notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- for children in Year 4 to Year 6 parents should ensure their child has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet (Appendix 2) and the Ipad contract (Appendix 3); and
- for pupils in Nursery to Year 3 parents should read and understand the terms on the acceptable use of the School's ICT systems and Internet and support their child accordingly.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7. Visitors and members of the community

Visitors and members of the community who use the School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 4).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education below Year 6 (RSHE)
- In **Pre Prep (Years 1 & 2)**, pupils will be taught to:
- use technology safely and respectfully, keeping personal information private; and
- identify where to go for help and support when they have concerns about content or contacton the internet or other online technologies.

Pupils in **Prep (Years 3 to 6),** will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour; and
- identify a range of ways to report concerns about content and contact.

By the **end of Year 6**, pupils will know:

- 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 includingawareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- what sorts of boundaries are appropriate in friendships with peers and others (including in adigital context); and
- how to respond safely and appropriately to adults they may encounter (in all contexts,including online) whom they do not know.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The School will raise parents/carers' awareness of internet safety in mailings, workshops and in information via our school portal. This policy will also be shared with parents/carers.

The School will let parents/carers know:

- what systems the School uses to filter and monitor online use; and when appropriate, the School will inform parents what their children are being asked to do online, including the sites they will be asked to access and who from the School (if anyone) their child will be interacting with online.
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

6. CYBER-BULLYING

6.1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSCHE education, and other subjects where appropriate.

All staff, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The School also sends information so they are aware of the signs and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the School will work to ensure the incident is contained. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3. Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils;
- is identified in the school rules as a banned item for which a search can be carried out; and/or
- is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher/ DSL / appropriate staff member
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it; and
- seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- cause harm;
- undermine the safe environment of the School or disrupt teaching; and/or
- commit an offence.

If inappropriate material is found on the device, it is up to the DSL / Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- they reasonably suspect that its continued existence is likely to cause harm to any person; and/or
- the pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **not** view the image; and confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- the DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people; and
- the School's Behaviour, Rewards and Sanctions Policy and the Searching Pupils Policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School's Complaints Policy and Procedure.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils from Years 4 to 6, parents/carers of all pupils, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet (Appendices 1 to 4). Visitors will be expected to read and agree to the School's terms on acceptable use if relevant.

Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, Governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 4.

8. PUPILS USING MOBILE DEVICES AT SCHOOL

Pupils may bring mobile devices into school only in Year 6 and with the permission of the Headteacher. The mobile phone must be given straight to a member of the Office team where is can be collected at the end of the day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the School's Behaviour, Rewards and Sanctions Policy, which may result in the confiscation of their device.

9. STAFF USING WORK DEVICES IN/OUTSIDE SCHOOL

Confidentiality

Nothing should be transmitted in an email or via clarion that you would not be comfortable writing in a letter or a memorandum.

- Email messages should be treated as non-confidential even if marked as private and confidential.
- Any information that is protected under the Data Protection Act should not be sent via email. This is information such as assessment data, dates of birth and any other personal information. Wherever possible, if this information needs to be shared, a link to such data, which is saved on the school server, should be sent in the email. In this way the data is still protected.
- If sending a link, then it should be sent as a Read-Only link and not as an editable one (which may expire after a certain date). Use of USB memory sticks or external hard drives should be avoided wherever possible.
- If the data must be sent outside the school's domain (@sthilarysschool.com) then it should be de-personalised and/or password protected. Such data should never be stored on a computer hard drive or any kind of portable storage. It should be noted that electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel cases.
- Staff should use initials rather than full names in emails.
- Messages sent through the Internet pass through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way.
- The school reserves the right to investigate emails for monitoring purposes, record keeping purposes, preventing or detecting crime, investigating or detecting the unauthorised use of the school's telecommunications system or ascertaining compliance with the school's practices or procedures.

Online Etiquette and Safety

- No offensive, obscene, demeaning or disruptive messages should be sent by email or retained on the School's ICT Systems.
- No message which you regard as personal, frivolous or potentially offensive to you or to any recipient should be placed on the system.
- If you receive mail containing material that is offensive or inappropriate in an office or school environment, then you must refer it to the Business Manager.
- No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another, unless agreed.
- All users must correctly identify themselves at all times. A user must not masquerade as another, withhold his/her identity, or tamper with audit trails.
- Under no circumstances should publication of opinions and untrue statements which adversely affect the reputation of a person or a group of persons be made. If such a statement is published on the Internet, including messages transmitted by email, an action for libel can be brought against those responsible.
- All staff should be aware that any documents, photographs, publications or original work that are produced as part of their employment belong to the School.
- Staff should dress appropriately when carrying out remote 'live' lessons.

- Staff should consider their environment when conducting live lessons and ensure that inappropriate posters, decorations or slogans are not present.
- Staff should treat live lessons as though they were in the classroom; with vigilant supervision of pupil's interactions, environments and noticeable well-being. They should be aware of the messages written and the chat facility. Any concerns should be raised with the DSL or Deputy DSL's.
- Staff should not use the break out Zoom facility and the chat rooms should not be left open and unsupervised on Showbie.
- Staff should use share screen with caution, making sure that they are not accidentally sharing emails/mark sheets or other confidential information.

Passwords

- Unique passwords will be issued to everyone requiring access to a particular resource. All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username.
- Passwords should not be shared. *
- Attempts to access or use any username which is not authorised to the user is prohibited.
- * During lockdown and the use of remote learning tools, Showbie passwords maybe shared to facilitate teaching and learning, and the smooth transition of class teacher should the need arise.

Viruses

- The school provides appropriate virus protection for all school computers.
- You must not run any 'exe' (executable files which install software) under any circumstances without the permission of the School ICT Manager
- No software shall be installed on any computer without the permission of the IT Manager.

Internet

- Access to the internet is restricted in line with relevant PREVENT keywords and filters prevent access to other unsuitable websites. You should refer any filtering issues to the ICT Manager.
- If you request that a particular website is unblocked, it is your responsibility to ensure that it contains appropriate material for use in school. If it does not, you must immediately request that it is excluded from viewing in school. The ICT Manager is responsible for actioning these requests.
- You may have access to the Internet during work time provided the sites are suitable to be viewed by children. Any improper use of the Internet is strictly prohibited. Improper use includes but is not limited to connecting, posting or downloading any information not deemed to be suitable to be viewed by children or attempting to disable or compromise security of information contained on the school's systems.
- Postings placed on the Internet may be traced back to the school's address. For this reason, you should make certain, before posting information, that the information reflects the standards and policies of the school. Under no circumstances should information of a confidential or sensitive nature be placed on the Internet.
- Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the copyright holder.
- Any online ordering must follow standard purchasing procedures.

- Subscriptions to news groups and mailing lists are only permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.
- All educational sites and clips must be watched in full before being shown or used in a lesson.

Emails

- Staff must use a secure and unique School email password that is not the same as any other online password. This is to prevent 'Credential Stuffing', a method in which cyber criminals can comprise a user's account using stolen details from another separate database.
- Any email received with an attachment (enclosure) or link should only be opened when the recipient is confident that the email is genuine.
- It is essential staff remain extra vigilant to Phishing email cyber-attacks. If any email is asking for personal information or includes external links, staff must ensure they are genuine. If in any doubt, staff must ask the ICT Manager to check for them.
- Extra care must also be taken when opening attachments and links even if the sender of the email is recognised as this can come from a compromised email account. Phishing attacks are used to steal a user's passwords and data. Never sign into your email or Microsoft Office 365 via a link included in an email. Always ask the ICT Manager if you are unsure if the email is genuine or from a hacked account.
- All business related emails should be sent via the school's email system. Personal email accounts must not be used. All emails sent externally should be professional in their approach, just as any letter sent out is written in a professional manner, as these reflect the image of the school.
- It is advised that emails are not read or responded to after 6:00pm for staff health and wellbeing. If this is unavoidable then it is recommended the email is saved in a staff members drafts folder and sent in the morning during school hours.

School ICT Equipment

- ICT equipment, including classroom and office computers, must be password locked when left unattended in the school. Any portable ICT equipment should not be left in vehicles, even in the boot.
- The laptop and iPad trollies must be kept padlocked.
- iPads must always be signed out using the Microsoft SharePoint booking system when in use so they can be accounted for.
- iPad charging cables and plugs must not be removed from the iPad charging cabinet for any reason as they are there to charge the class iPads for lessons only. If a cable is needed, one can be temporarily loaned by the ICT Manager.
- ICT equipment loaned to an individual remains the property of the school and must be returned when a member of staff leaves the employment of the school or when requested to do so by any member of the SLT or the ICT Manager.
- The school will provide all ICT equipment considered necessary for staff to fulfil their role effectively. This equipment should never be used as a personal device.

Back-up Arrangements

All Staff who use ICT as part of their job are able to save their work onto the school server. The server is backed up on a daily basis to a secure off-site location.

Files and data must not be saved locally on the school computer – and should be saved in the user's home folder (N:Drive) or in the shared folders on the network. This way the data is backed up and can be recovered. Files, documents and data saved on a user's desktop or documents folder on the computer are not backed up and cannot be recovered if the computer or device is damaged or faulty.

Staff should make use of Microsoft OneDrive to store and backup data. A unique and secure password must be used. USB storage devices are not secure and must not be used.

Offsite Access to School Data
All teaching and admin staff can access the school network from a home PC and therefore work directly on files or the School Management System. Staff should ensure that sensitive information, including documents and images relating to children, remains on the server and is not copied onto home computers and that all prudent measures are taken to protect information contained on the network or School Management System.

Laptops, iPads and Portable Storage Devices
The school provides laptops or iPads to staff where appropriate. Staff with a laptop may store information that is not sensitive (such as general class planning, policies, general documentation or correspondence) on the hard drive but any sensitive information must be stored in accordance with the offsite access procedure above. The PIN code of iPads must remain confidential if email is configured on the device. Work iPads must be set to have a 6-digit access code rather than the 4-digit standard access code. As a matter of good practice the school recommends that staff should change the access code to their own personal devices to something more secure than the standard 4-digit code, and that they **must** do so if they have access to their work emails via such devices.

Hardware
All ICT hardware (Note 2) should be purchased through the ICT Manager in order to ensure that an up-to-date ICT asset register is maintained for the school. Deliveries should be checked by the ICT Manager and set up/installed where necessary before being given to the member of staff who requested the item. All ICT hardware should be security marked with the school's inventory labels by the ICT Manager.

Software
It is the policy of the school to respect all computer software copyrights and to adhere to the terms of all software licences. It is the legal obligation of the school and its employees to comply with copyright laws and respect the intellectual property rights of others. It is therefore expressly forbidden for any employee to have possession of unlicensed software on school premises or use unlicensed software on school computers. Users may not duplicate any licensed software or related documentation unless expressly authorised to do so by agreement with the licenser. Unauthorised duplication of software may subject users and/or the school to both civil and criminal penalties under the Copyright Designs and Patents Act 1988 (and related EC directives). According to the Copyright, Designs and Patents Act 1988, infringement of software is actionable in the civil courts. Users who make, acquire or use unauthorised copies of software will be disciplined as appropriate under the circumstances. Such discipline may include dismissal.

To purchase software, users must order through the ICT Manager, who is also responsible for registering software with the software publisher. The ICT Manager will also ensure that the software is compatible with the school system.

Digital Photos/Videos

All photos taken in school or on school activities must be relevant and appropriate and taken on school owned equipment. This is for the protection of staff and children. Staff should not use their own cameras, video equipment or mobile phones to take images of children. Photos should be stored on school computers and removed from the camera as soon as possible. Photos and videos should only ever be displayed in accordance with the permissions of the parents and full names should never be attributed.

Any photographs of children used in electronic communications (e.g. Twitter, Facebook, the school website) should only include first names and first letter of surname. Live streaming of pupils will not take place at any events onsite or offsite. Any misuse of photographs will be reported to the Designated Safeguarding Lead.

Any external photographers or video recordists invited by the school will have a clear brief and not be left alone with any pupils. All parents will be informed.

Social Networking (e.g. Facebook, Twitter, YouTube)

Employees should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or 'friends only' level and therefore they should not assume that their entries on any website will remain private. When using social networking sites staff must be aware of the dangers and pitfalls both to themselves and to the reputation of the school. Communications should remain respectful in tone at all times.

The school strongly recommends that staff do not contact children or ex-pupils under the age of 18 from the school using these sites. This is to protect the staff member's professional integrity and the integrity of the school. Examples of inappropriate use of these websites includes making any derogatory, offensive, discriminatory or defamatory comments about the school, its employees, contractors, suppliers, customers or clients. Employees who are discovered to have brought the school into disrepute in any way, whether inside or outside the workplace, may face serious disciplinary action under the School's disciplinary procedure.

Staff using school social media outlets e.g. the school's Twitter or Facebook accounts, will always adhere to the permissions given (or not) by parents for the use of images of their children in such circumstances.

The School reserves the right to monitor staff communications in order to: -

- establish the existence of facts
- ascertain compliance with regulatory or self-regulatory procedures
- monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes
- prevent or detect crime
- investigate or detect unauthorised use of the School's telecommunication system
- ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations
- gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

Personal Mobile Phones/Devices

The school allows staff to bring in personal mobile phones and devices for their own use. However, these should only ever be used in non-contact time and should never impact on school business. The school office number should be given to family or dependants in case of emergency. They must be stored in a cupboard or drawer that is not accessed by the children and kept on silent. Staff must only use these when children are not present. The only exception to this is if a mobile phone is needed to monitor a specific medical condition such as diabetes. This would need to be communicated in writing to the Headteacher and DSL.

All mobile devices accessing the internet using mobile data (3G/4G/5G) must be used in an appropriate manner for the work place environment.

Under no circumstances should these devices be charged on the premises due to electrical safety testing requirements. Similarly, the school allows staff use of school equipment to access personal emails, internet etc. as long as this does not impact on school business. This applies equally to all school staff.

Staff should never give their personal mobile number to parents.

The school is not responsible for the loss, damage or theft of a personal mobile device on school premises. It is not permissible to record images or sound clips of pupils or staff on any personal device.

The School has a wireless system for use by school devices. Any requests for access to the wireless system for a personal device should be directed to the IT Manager but will only be authorised for work purposes.

Smart Technology

Despite the obvious distraction that these devices can pose, smart watches are internet and camera enabled and therefore present the same concerns as mobile phones in terms of safeguarding. Parents should not allow their children to wear a smart watch to school**.** Staff should be aware that if they do wear a smart watch it should only be used in its watch capacity when in contact with pupils.

Safeguarding Policy Restrictions for the use of Mobile Phones in EYFS

- Nursery staff store their phones in a locked cupboard in Nursery, or in the Kindergarten office
- Kindergarten staff store their phones in the Kindergarten office
- Reception staff store their phones in the locked cupboards in each classroom
- All EYFS staff use their phones when there are no children present, either in the staff room, empty classroom or the Kindergarten office
- Staff have access to their phones during their breaks or non-contact times, providing there are no children present
- Staff are asked not to check their Smart watches until the times outlined above

Please also see: Safeguarding and Child Protection Policy

Security of Information

In line with the Data Protection Act it is essential that all staff manage sensitive information (Note 1) in a secure manner. Any such information **must be** saved to the school server. Such data **must not, under any circumstances,** be stored on devices not belonging to the school.

Note 1 – Definition of Sensitive Information

Sensitive information includes annual reports, annual review paperwork, SSPs, PIPS data or any other documentation relating to specific children and giving personal details (name, address, date of birth etc.). This also includes images of children taken by still camera, video camera, mobile phone etc. Sensitive information also relates to documentation relating to members of staff and giving personal details.

Note 2 – Definition of Hardware

ICT Hardware includes all computers (desktops, laptops, tablets and netbooks) digital cameras (still and video), visualisers, printers, microphones, projectors, interactive whiteboards, robotic and any other peripheral devices such as MP3 players etc.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in the Behaviour, Discipline and Sanctions Policy and terms of acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individualcircumstances, nature and seriousness of the specific incident.

The School will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. An online Educare course on Cyber safety is regularly taken by all staff.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- children can abuse their peers online through:
    - abusive, harassing, and misogynistic messages;
    - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups; or
    - sharing of abusive images and pornography, to those who don't want to receive suchcontent; and
- physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse;
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks; and
- develop the ability to influence pupils to make the healthiest long-term choices and keepthem safe from harm in the short term.

The DSL and Deputy Designated Leads will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding (Child Protection) Policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 6 and a Filtering and Monitoring log in Appendix 7.

This policy will be reviewed every year by the Headteacher, DSL and IT Manager. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. LINKS WITH OTHER POLICIES

This E-Safety Policy is linked to our:

- Safeguarding (Child Protection) Policy;
- Behaviour, Discipline and Exclusions Policy;
- Staff disciplinary procedures;
- Privacy Notice;
- Complaints Policy and Procedure;
- Remote Learning Policy
- Remote Working Mobile Device Policy
- Photographic Images of Children Policy

APPENDIX 1: ACCEPTABLE USE AGREEMENT OF THE INTERNET

PARENT CONSENT FORM

(All parents will be required to sign this on entry)

St Hilary's Prep School

Acceptable Internet Use

The computer system is made available to pupils at St Hilary's School to further their education. This statement is drawn up to ensure the safety and privacy of pupils when using the Internet and to protect the schools' computer system.

• All Internet access at St Hilary's School is filtered through a proxy server to screen undesirable sites at source.
• The Internet can only be accessed with the permission of a teacher and when that teacher is present in the classroom.
• All Internet activity should be appropriate to school work.
• Pupils may not attempt to access any inappropriate or unacceptable material.
• Internet use and sites visited are subject to scrutiny by staff.
• Children will not engage in conversation or dialogue with other users on the Internet without permission or supervision from their teacher.
• Children and staff must never reveal their or any other person's, personal details, or home addresses and telephone numbers on the web or in dialogue with other Internet users.
• All E-mail to pupils will be moderated by a member of staff.
• No meetings should be arranged by pupils as a result of electronic contact.
• Any child finding themselves uncomfortable or upset by anything they discover on the Internet will report it to a teacher immediately.
• Newsgroups or Chat lines must not be used.
• No goods or services must be ordered.
• The downloading of files is restricted to staff only.
• Copyright of materials must be respected.
• Pupils will only be referred to by their first name on the school web pages.
• Any images of pupils will not be labelled with their full name.
• Activity that threatens the integrity of the school IT system, or activity that attacks or corrupts other systems, is forbidden.
• Pupils must be aware that information taken from the Internet may not always be true or correct.
• Parents will work in close collaboration with the School to support online safety and social responsibility when using devices at home.
• Parents will speak with their child/ren regarding:

- ✓ Having permission from the teacher before using technology
- ✓ Only using websites that a teacher or adult has allowed them to use
- ✓ Using School devices for School work only
- ✓ Being kind to others and not upsetting or being rude to them
- ✓ Looking after the School's ICT equipment and telling a teacher straight away if something is broken or not working properly
- ✓ Only using the username and password they have been given

- ✓ Trying their hardest to remember their username and password
- ✓ Never sharing their password with anyone, including their friends
- ✓ Never giving personal information (my name, address or telephone numbers) to anyone without the permission of their teacher or parent/carer
- ✓ Saving their work on the correct digital platform
- ✓ Not taking images of others without their permission
- ✓ Logging off or shutting down a computer when they have finished using it
- ✓ Telling their teacher immediately if:
- ✓ They click on a website by mistake
- ✓ They receive messages from people they don't know
- ✓ They find anything that may upset or harm them or my friends

I have read the Acceptable Internet Use Policy above and give permission for my child to use the Internet at St Hilary's School.

Please type your full name below to confirm that you agree to the above, unless the school is notified to the contrary in writing

APPENDIX 2: YEARS 4 TO 6 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in this acceptable use agreement.

When I use the School's ICT systems and use the internet in School I will:

- Always use the School's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number toanyone without the permission of my teacher or parent/carer
- Tell a teacher (or appropriate adult) immediately if I find any material which might upset, distress or harm me or others
- Save my work on the correct digital platform
- Always log off or shut down a computer when I've finished working on it
- If I have arrangements to print work I will check with my teacher before sending to print
- Ensure my iPad is ready and charged for the working day

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the School's network using someone else's details
- Take images of others without their permission
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone into School:

- I will hand it in on arrival to the School Office. Mobiles can only be brought in to school in Year 6 and the Headteacher's permission must be sort first.

I agree that the School will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of School staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and for using personal electronic devices in School, and will make sure mychild understands these.

Signed (parent/carer):	**Date:**

APPENDIX 3: Year 4- 6 IPAD CONTRACT

iPad User Contract

Your iPad is a wonderful educational tool. You may use your iPad to take class notes, record and complete homework, and to check messages, email, announcements and calendars.

However, there are some simple rules you must follow when using your iPad in school.

1. ***I will bring my iPad to school every day, fully charged.***
2. ***I will charge my stylus at least once a week or when a red light appears.***
3. ***I will keep my iPad healthy by installing updates regularly.***
4. ***I will keep my school work safe by backing up my iPad files.***
5. ***I will keep my iPad passcode private.***
6. ***I will not use the iPad camera without obtaining permission from a member of staff first.***
7. ***I will not open any app or game during a lesson without obtaining permission first.***
8. ***I will keep the iPad sound muted at all times, unless given permission to use it by a teacher.***
9. ***I will not use the internet during lessons without obtaining permission first.***
10. ***I will follow and adhere to the ACCEPTABLE USE AGREEMENT, the PUPILS E-SAFETY AND ACCEPTABLE USE POLICY and the IPAD CONTRACT RULES at all times.***

APPENDIX 4: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, 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 follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the DSL.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of e-safety: smart technology/ mobile phones / devices at school.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system within school.
- 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 or laptop 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 and Customs.
- I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.
- 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 alert the DSL/ appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way to the DSL.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies 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 e-safety policies.

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

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

Full Name ..... (printed)

Job title / Role .....

APPENDIX 5: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Comment**
Name of the person who has lead responsibility for online safety in school?	
Describe the ways pupils can abuse their peers online?	
What should you do if a pupil approaches you with a concern or issue?	
When did you last read the School's acceptable use agreement for staff, volunteers, Governors and visitors?	
When did you last read the School's acceptable use agreement for pupils and parents/carers?	
Can you describe (in simple terms) the filtering and monitoring systems on the School's devices and networks?	
What are your roles and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the School's ICT systems?	
What is the School's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

To be used annually with staff

APPENDIX 6: ONLINE SAFETY INCIDENT REPORT LOG

ICT Incident Log

Name of Pupil: _____ **M/F** **Class:** _____

Logged by: _____ **Date:** _____

EAL/SEND/ETHNICITY _____

Where did the incident take place? e.g classroom/playground/corridor/cloakroom/out on a trip/out of school

When did the incident take place? e.g playtime/lunchtime/before school/during lessons/assembly/out of school

Brief description of Incident: (You may add communications/conversations here including pupil voice)
Action Taken (Please circle) ◊ Children/Child concerned interviewed ◊ Class Teacher informed ◊ Head/Deputy informed ◊ Parent/Carer informed ◊ Meeting with Parent/Carer Arranged ◊ If you are concerned that this has escalated to 'safeguarding' please speak to the DSL/DDSL immediately. ◊ E-Safety/Online Coordinators ◊ Police ◊ Prevent ◊ CEOPS ◊ Other
Consequences/further action including analysis of future risk, resolution and outcome:

APPENDIX 7: FILTERING AND MONITORING LOG

Incident Record	Date	Notes
Harmful and Inappropriate Content reported		
Cyber Attack		
Data breach of Personal Information		
Staff report of ICT Safeguarding Concern		
Parent report of ICT Safeguarding Concern		

Author: Business Manager/Head of Computing/IT Manager/DSL
Read & Approved by: The Headteacher and St Hilary's Senior Leadership Team.
Read & Shared: with all staff at St Hilary's School.
Reviewed: June 2019, July 2020, September 2020, January 2021, June 2021, June 2022, July 2023, September, November 2023, December 2023
Next Review Date: June 2024
Persons responsible: Mr Mark Strickland (ICT Manager), Mr James South (Head of Digital Learning), Mrs Julia Ranger (Head of EYFS) Mrs Gemma Mitchell (Deputy Head)