St Hilary's School
E-Safety Policy
(including Photography, Use of Mobile & Smart Technology)

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

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.'

Purpose and Scope

St Hilary's School Trust Limited ("the school") expects all its ICT facilities to be used in a responsible manner. These facilities are provided by the school for educational and administrative purposes.

It is the responsibility of each employee to ensure that this technology is used for business purposes and in a manner that does not compromise the School or its employees in any way. They must also ensure that their own behaviour with regards to ICT is professional at all times.

Staff have a responsibility to ensure that sensitive information, including documents and images relating to children, is protected. Additionally, they must ensure that school ICT equipment is used, stored or transported in a secure manner and that school data is not stored on personal devices.

This policy should be read in conjunction with 'Photographic Images of Children Policy' and 'Remote Working Mobile Device Policy.'

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 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 Teams 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.

Teaching Children How to Keep Safe

Staff have a responsibility to ensure that pupils remain safe online whilst at school. Please see the school's Safeguarding/Child Protection Policy and Digital Learning Policy.

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Digital Learning curriculum/PSCHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind children about their responsibilities through the Pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff (including those on work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides online safety advice, guidance and training for parents.

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

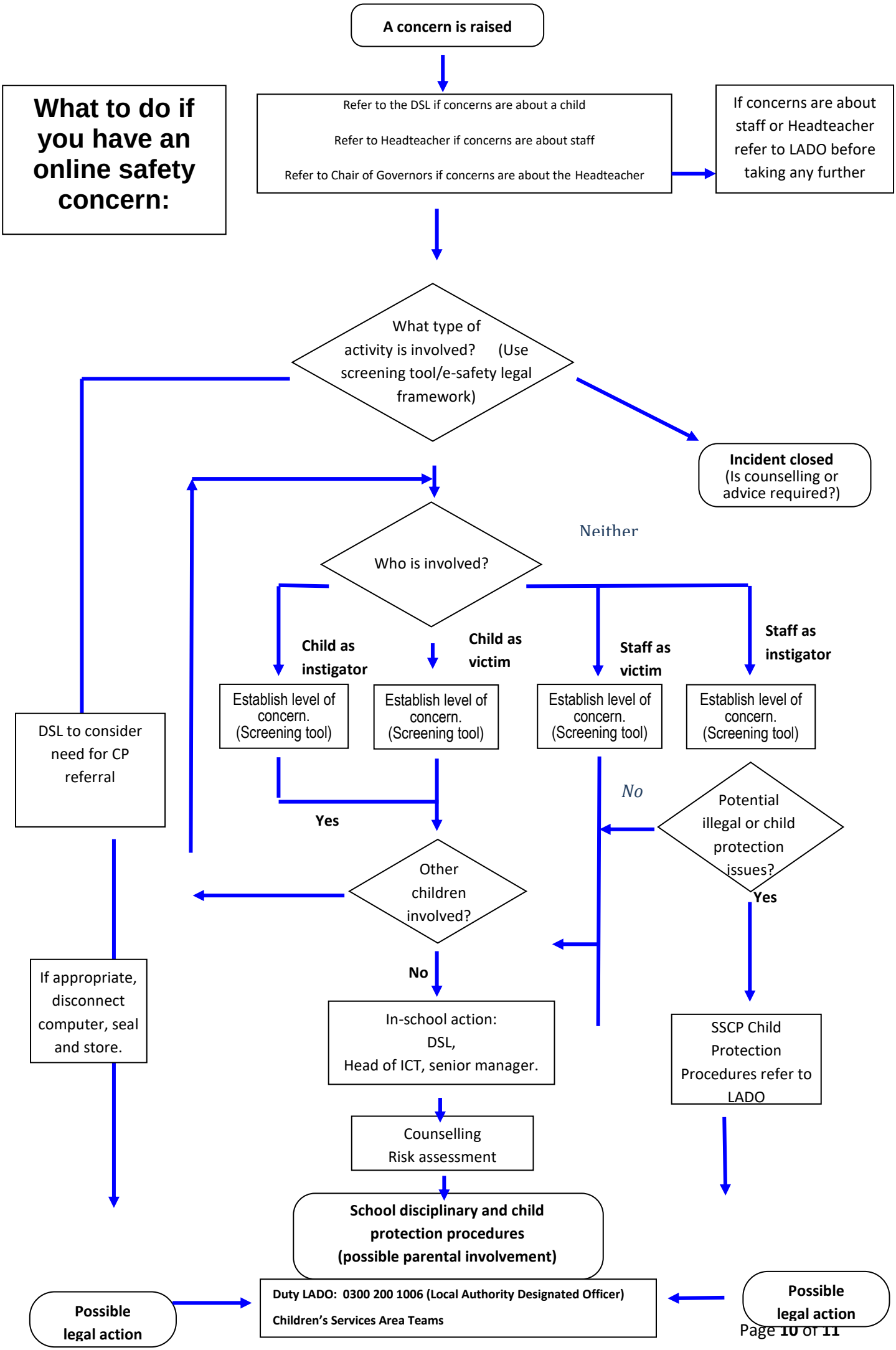
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police and Internet Watch Foundation.

What to do if you have an online safety 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
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)