Online Safety and Acceptable Use of ICT and the Internet Policy

Original Author/Person Responsible	**E Ross** **(G Fricker & L Oram)** **July 2021**
Review Frequency	**Every two years** ***Subject to LEA and/or national policy change***
Review Group	**Full Governing Body**
Chair of Governors Signature	
Reviewed **Amendments/Notes**	
Next review date	**July 2023**
Related Policies - the policy should be read in conjunction with these policies	Remote Learning Policy Child Protection and Safeguarding Policy Accessibility Policy Data protection Policy Staff Disciplinary Policy Behaviour policy

Abbreviations and Definitions

ICT Information, Communication Technology - includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

Users - anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

Personal use - any use or activity not directly related to the users' employment, study or purpose

Authorised personnel- employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

Materials - files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

Contents

1. Introduction and Rationale behind the use of ICT
2. Aims of the Policy
3. Relevant legislation and guidance
4. Unacceptable use
    - 4.1 Exceptions from unacceptable use
    - 4.2 Sanctions
5. Staff (including governors, volunteers, and contractors)
    - 5.1 Access to school ICT facilities and materials
    - 5.2 Use of phones and email for communication purposes
    - 5.3 Personal use
    - 5.4 Personal social media accounts
    - 5.5 Remote access
    - 5.6 Monitoring of school network and use of ICT facilities
6. Pupils Access to ICT facilities and the Internet
    - 6.1 Pupils' home-school agreement
    - 6.2 Online Safety Curriculum
    - 6.3 Management of pupils using ICT and the internet for communication
7. Parents
    - 7.1 Access to ICT facilities and materials
    - 7.2 Communicating with or about the school online
    - 7.3 Education of Parents/Carers on Online Safety
8. Data security

8.1 Passwords

8.2 Software updates, firewalls, and anti-virus software

8.3 Data protection

8.4 Access to facilities and materials

8.5 Encryption

9. Internet access

9.1 Filtering and monitoring

10. Reporting Incident

11. School Website

12. Appendix 1: Facebook cheat sheet for staff

13. Appendix 2: Acceptable use of the internet: agreement for parents and carers

14. Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

15. Appendix 4: Web based resources

1. Introduction and Rationale behind the use of ICT

ICT is an integral part of teaching and learning at Henleaze Infant school. It is used by staff and children as a tool across all areas of the curriculum, in particular for Technology in EYFS and the Computing Curriculum in KS1, ICT is used to enhance and stimulate children's learning, as well as to aid communication and for pastoral and administrative functions.

We need however to ensure that children and staff engage in safe practices when accessing the internet and are aware of the issues involved in its use. Managing and minimising the risks is key to ensuring safe practice.

Why is internet use important?

- The Internet enhances the curriculum and is used as an effective tool for communication, motivation and administration.
- The effective use of the internet enriches and extends learning activities and provides children with essential skills they need.
- It allows children to learn and use the necessary skills to locate and use information.

2. Aims of the Policy

While we value the positive impact of ICT and internet usage on children's education, we recognise that it's usage also poses risks to data protection, online safety and safeguarding.

According to 'National Online Safety' the definition of Online Safety is:

"In simple terms, online safety refers to the act of staying safe online. It is also commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets.

Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardise their personal information, lead to unsafe communications or even effect their mental health and wellbeing.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- Breaches of this policy may be dealt with under our Disciplinary policy.

3. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for schools

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below). Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion, consent needs to be sought.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's Disciplinary policy.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school IT services keep a record of all staff who are granted internet access and access to our ICT facilities. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files
- Access to the internet

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. The system automatically requires these passwords to be updated regularly. Staff are required to keep their log in details and passwords for this private.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the headteacher or school business manager.

5.2 Use of phones and email for communication purposes

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the headteacher and school business manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. If staff need to use their personal phones to contact parents they should change the settings to make the caller ID hidden.

School phones must not be used for personal matters, without permission from the headteacher.

5.3 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher or school business manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- It only takes place during breaks and out of work hours.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 9.1). Where breaches of this policy are found, disciplinary action may be taken.

Staff on occasion may want to use their personal devices, such as mobile phones and tablets in school working hours to support with their role (for example, to play music). Permission must be sought from the headteacher or a member of SLT to do this.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.4 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.5 Remote access

We allow staff to access the school's ICT facilities and materials remotely via Google Drive. Staff are required to keep their log in details for these private.

This is managed by the Headteacher, the Computing curriculum lead and Assistant Headteacher.

Security arrangements have been overseen by Bristol City Council to ensure that it has been set up in a secure way.

Staff are only able to access this using their school email addresses.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The school's data protection policy can be found in the policy section of the school website.

5.6 Monitoring of school network and use of ICT facilities

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

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs

- Any other electronic communications

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

The school monitors ICT use in order to:

- Obtain information related to the legitimate business interests of the school
- Safeguarding of our pupils and staff in accordance with Keeping Children Safe in Education 2020
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils Access to ICT facilities and the Internet

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. Neither the school nor Bristol County Council can accept liability for the material accessed, or any consequences of internet access.

The school will take all reasonable precautions to minimise risks when using online technologies through a combination of Online Safety education, filtering and monitoring children's online activity and reporting incidents, including following Child Protection procedures where appropriate.

Central to minimising the risks of internet and ICT usage in school is that:

- Pupils will only use ICT under the guidance of staff
- Pupils will use the internet under supervision of staff and will be clearly shown what websites they can access.

6.1 Pupils' home-school agreement

The agreement will include the acceptable use policy and guidance for video, sound and images for web publication. The agreement will be signed by parents on entry to the school before pupils are allowed to access the internet.

6.2 Online Safety Curriculum

Pupils will have specific lessons, within the Computing and PSHE curriculum to learn about Online Safety. These lessons will be carried out during the beginning of a new school year and are revisited in the week of 'Safer Internet Day'. Teaching content and delivery will be planned to suit the age of the children and will cover the aims set out in the National Curriculum for Computing which states that:

- At KS1: 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.

Pupils understanding of online safety will also be reinforced throughout the year by:

- Having Online Safety Rules displayed in classes and these messages will be reinforced and recapped when using ICT and the internet, to remind children of the code of conduct for internet.
- Being taught how to access approved websites, specifically relating to tasks/activities they are doing.
- Being taught that they can should ask a member of staff (or 'a trusted adult' so the messages relate to home usage) straight away if they see something that they do not like on the internet.
- The school will conduct pupil surveys about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them to review the content and relevance of the Online Safety Curriculum

6.3 Management of pupils using ICT and the internet for communication

- Pupils will be taught that e-mails need to be written in a polite and courteous manner, in line with our School Online Safety Rules.
- Pupils will be taught about safety issues as part of our Online Safety Curriculum if using an email system outside school.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the home-school agreement in appendix 2.

7.3 Education of Parents/Carers on Online Safety

The school supports parents and carers on understanding the importance of Online Safety and how to manage online safety risks at home by:

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school Website.
- Parents will be given information via the school website and curriculum updates to inform them of how ICT is used in school, its benefits, and how to promote e-safety at home.
- Information is always available on our school website. This includes links to different online safety websites such as:
  - Safer Internet https://www.saferinternet.org.uk/
  - NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/
  - SWGfL https://swgfl.org.uk/online-safety/
  - Common sense media https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Parents will be invited to events where up to date information is given around Online Safety at home. These are often in partnership with the Junior school or local schools.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

If your school allocates passwords, or requires regular password updates, explain this here.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Add a link to your school's data protection policy here, or explain where it can be found.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the headteacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the headteacher.

9. Internet access

The school wireless internet connection is secured.

Pupils will only have access to the internet under staff supervision and steps will be taken to minimise risks to pupils when using the internet, including Online Safety curriculum and filtering and monitoring (Section 9.1).

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher. The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

9.1 Filtering and Monitoring

The Prevent Guidance, released in response to the Counter-Terrorism and Security Act 2015, requires schools to have filtering of ICT in place to ensure children are safe from terrorist and extremist material when accessing the internet in school.

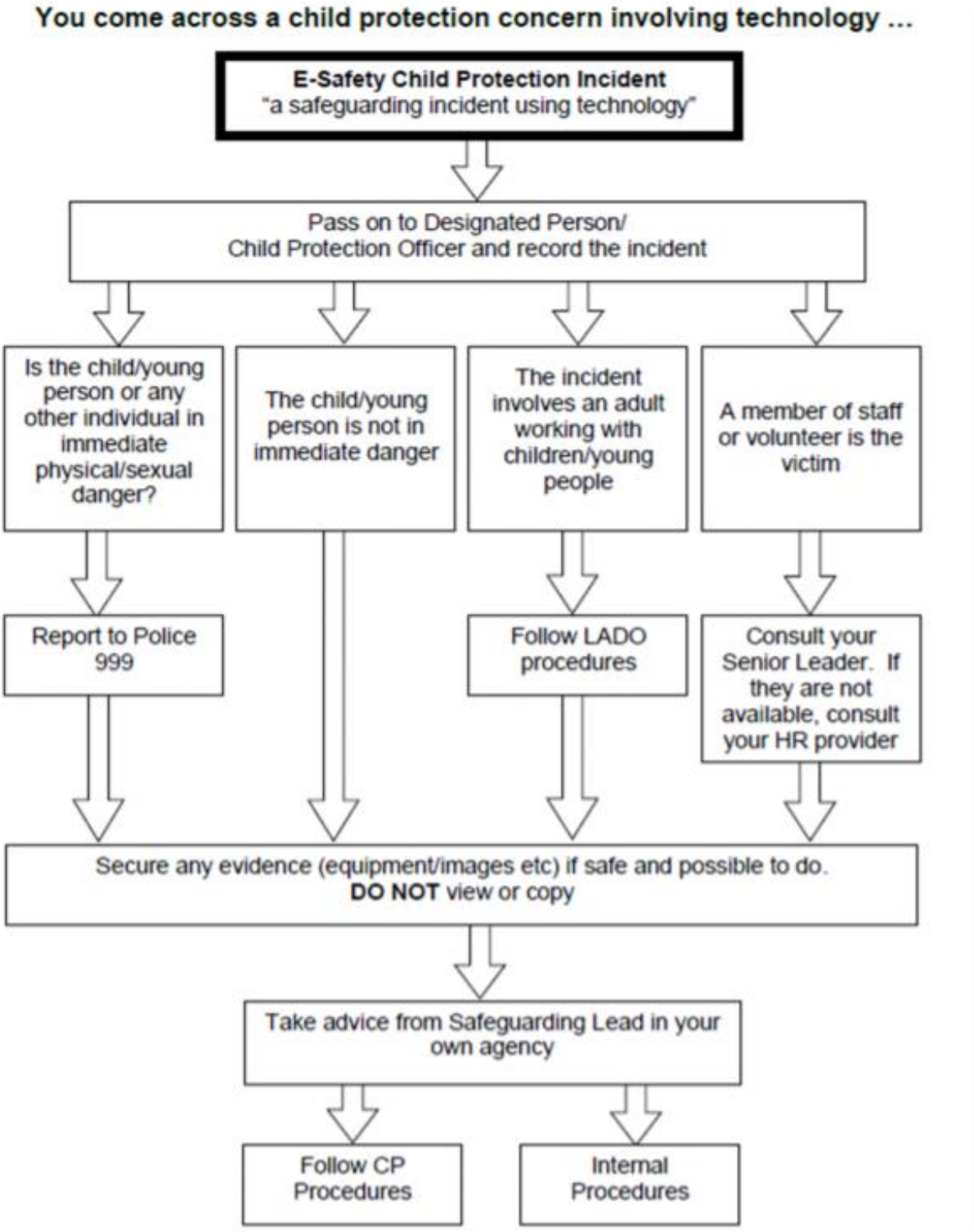
Henleaze Infant School uses Trading with schools as part of Bristol Local Education Authority to deliver internet access to the school and support with the maintenance of ICT equipment.

This service filters internet access by cross-referencing all website requests against a banned list which is continually updated. In addition to this schools can permit or deny sites that they feel appropriate for the duration they choose.

10 Reporting Incident

The school will work in partnership with parents, Bristol County Council and Department for Education, Schools and Families to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the headteacher as well as the Bristol City Council ICT Helpdesk on 0117 9037999 (cyps.it.helpdesk@bristol.gov.uk)

Staff and Governors are made aware of the UK SAFER INTERNET CENTRE HELPLINE 0844 3814772. The following steps should be taken if you have a child protection concern involving ICT and the internet:


You come across a child protection concern involving technology ...
E-Safety Child Protection Incident
"a safeguarding incident using technology"
Pass on to Designated Person/
Child Protection Officer and record the incident
Is the child/young person or any other individual in immediate physical/sexual danger?
The child/young person is not in immediate danger
The incident involves an adult working with children/young people
A member of staff or volunteer is the victim
Report to Police 999
Follow LADO procedures
Consult your Senior Leader. If they are not available, consult your HR provider
Secure any evidence (equipment/images etc) if safe and possible to do.
DO NOT view or copy
Take advice from Safeguarding Lead in your own agency
Follow CP Procedures
Internal Procedures

11. School Website

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information to our pupils and parents, promote the school to prospective pupils and families and publish the statutory information required by the Department for Education. The website will also be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

The school will ensure that every child in their care is safe,and that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website. The following precautions should be adhered to:

- Staff will only be given access to passwords required to update the website who have read and understood the guidance and rules around its use
- The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not be published alongside their name or any other means of enabling the individual to be clearly identified.
- Pupils' full names will not be used anywhere on the website, first names may be used but not alongside a photograph.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website.
- Videos and images may be published on different websites or media of children in order to showcase things that wouldn't be able to be done in another way (e.g. school plays on Youtube, as an unlisted video, as a result of Covid restrictions). This will only be done with parental permissions.

12. Monitoring and review

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

Appendix 1: Facebook cheat sheet for staff

If you have a social media policy, adapt this in line with that policy. You may decide to hand this cheat sheet out to your staff as a standalone document and remove it from here. If so, renumber the following appendices and check for references to appendix 1 in the policy.

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead

2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional

3. Check your privacy settings regularly

4. Be careful about tagging other staff members in images or posts

5. Don't share anything publicly that you wouldn't be just as happy showing your pupils

6. Don't use social media sites during school hours

7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there

8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)

9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this

Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings again, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

Save evidence of any abuse by taking screenshots and recording the time and date it occurred

Report the material to Facebook or the relevant social network and ask them to remove it

If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels:

- Our school website
- Our official FHIS Facebook page
- Email/text groups for parents (for school announcements and information
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	Date:

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

Henleaze Infants' School Acceptable Use of ICT Agreement

- I understand that the network is the property of the school and agree that my use must be compatible with my professional role.
- I understand that the school ICT systems may not be used for private purposes, without the specific permission from a member of the SLT.
- I understand that personal mobile phones may only be switched on during out of hours and lunchtimes, without specific permission from a member of the SLT.
- I will not take photographs with any other camera than the school cameras. This includes mobile phone cameras which will not be used for taking photographs of any children and families within the setting, without specific permission from a member of the SLT.
- I understand digital images needed for professional purposes may be stored for a period of three years. After this time I agree to be responsible for deleting them.
- I will ensure that my electronic communications with parents and carers are compatible with professional role and cannot be misinterpreted.
- I will embed the school's Online Safety curriculum into my classroom practice.I
- will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to will not compromise my professional responsibilities.
- I will respect copyright and intellectual property rights.

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) andSchool Business Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 4: Web based resources

KidSmart http://www.kidsmart.org.uk/: SMART rules from Childnet International and Know It All for Parents

UK Safer Internet Centre https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline

National Online Safety https://nationalonlinesafety.com/

Childnet International http://www.childnet-int.org/: Guidance for parents, schools and pupils

DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/

Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Websites

South West Grid for Learning – Safe www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining internet dangers and how to stay in control.

For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online

School Top Tips on how to stay safe online
enle