White Laith Primary School
E-SAFETY & ACCEPTABLE USE POLICY
February 2024

Review Date: February 2025

Safeguarding

At White Laith we are committed to providing a caring, friendly and safe environment for all of our pupils so they can learn in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by or invited to deliver services at White Laith. We recognise our responsibility to safeguard and promote the welfare of all our pupils by protecting them from physical, sexual or emotional abuse, neglect, bullying and harmful inappropriate online material. We also exercise this responsibility by educating our children so that they grow in their understanding of their rights and responsibilities to themselves and others, in safety consciousness, and, in their maturity and abilities to keep themselves and others safe. We perceive this to be part of our role in promoting British values.

1. Aims

   To ensure teachers and pupils use electronic technologies in and outside school in a way which will keep them safe without limiting their opportunities for creativity and innovation.

   To protect school hardware and software from attack by computer viruses and unscrupulous people, who may wish to cause disruption or commit illegal acts.

   To protect teachers and pupil's personal information.

2. Introduction

   2.1. White Laith makes widespread use of modern technology in the belief and understanding that it can develop and enhance many aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

   2.2. The increased use of technology at work and at home exposes people to a number of risks and dangers. It is essential that children are safeguarded from potential harmful and inappropriate online material.

   2.3. In its simplest form e-safety is about ensuring people use electronic technologies in a way which will keep them safe with minimal effect of their opportunities for creativity and innovation. We promote an effective whole school approach to online safety to educate pupils, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

   2.4. The breath of issues classified within online safety can be catergorised into four area of risk:

      2.4.1. **Content:** being exposed to illegal, inappropriate or harmful content, e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti- Semitism, radicalization and extremism.

      2.4.2. **Contact:** being subjected to harmful online interaction with other users; e.g. 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 or other purposes.

      2.4.3. Conduct: personal online behavior that increase the likelihood of, or causes, harm for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

      2.4.4. Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

   2.5. Using the Internet to seek information and communicate with others is an important life skill. It is essential to equip them with the skills, knowledge and understanding to use the internet safely.

   2.6. This policy

      - Applies to all users of ICT equipment whilst on school premises.
      - Applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.
      - Should be read in conjunction with other school policies including, safer working practice, child protection, behaviour and anti-bullying, Acceptable use policy - E-safety guidance for staff.

   2.7. This policy will be reviewed on an annual basis.

3. Responsibilities

   3.1. The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

   3.2. Everyone who uses IT connected with the school has a responsibility to have a regard for e-safety.

3.3. In line with requirements of the PREVENT duty this policy pays due regard to the need to prevent people from being drawn into terrorism. Filtering ensures that content is blocked and this is monitored by the e-safety leader and our technician.

3.4. The Governors and Management of the school have the responsibility to ensure that all employees and pupils are aware of e-safety concerns and procedures, and that they receive training to raise their awareness of the issues involved.

3.5. The teaching staff are responsible, as part of the statutory requirements of the curriculum, for the teaching of e-safety.

3.6. Although the ultimate responsibility lies with the Governing Body and the Head teacher, the school will nominate
- an E-Safety Leader: Mr. Michael Sheerin
- a Governor with responsibility for e-safety issues: Mr. Greg Potter
- a member of the senior management team to deal with e-safety issues and e-safety complaints in particular: Mrs. Nicola Sheerin

3.7. The E-Safety Leader will
- Oversee the development and implementation of this policy.
- Advise the school management on e-safety issues.
- Liaise with the PSHE leader (online safety, Prevent)
- Lead the teaching of e-safety to all classes.
- Advise staff on e-safety teaching and learning resources.
- Answer questions or concerns about e-safety issues anyone connected with the school may have.
- Be informed of infringements of the e-safety policy and rules, including accidental infringements, and act upon these appropriately.
- Pass on to the Head teacher any complaint or evidence received concerning individual pupils or staff misuse of electronic technologies.

4. Teaching and learning

4.1. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

4.2. The school Internet access will include filtering appropriate to the age of pupils. *(The filtering service is provided by ISP, Schools Broadband)*

4.3. Pupil's access the internet will be guided by a school "Internet/Online Code", which will be displayed in all classrooms and the IT suite. See appendices A and B.

4.4. Pupils will access the internet on a PC or Chromebook using Google Chrome. On opening an internet browser, they will be directed to the school homepage "dashboard". This dashboard will present direct links with main websites used for teaching and learning e.g. Purple Mash, SWIGGLE, and Kiddle. Other website links can be stored in the folder called "Web-links" in the Exercises (E) drive on the school curriculum network.

4.5. Pupils will access the internet on an iPad using a 'webclip' showing the school dashboard.

4.6. Pupils will be given clear objectives for Internet use. **Aimless web browsing is not allowed.**

4.7. As part of the computing curriculum pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation. They will also be educated in complying with copyright law when using Internet derived materials.

4.8. Pupils will be taught how to report unpleasant Internet content to a trusted adult, or if appropriate, using the CEOP Report Abuse on the school pupil safety page.

5. Equal Opportunities

The school believes that it is essential that opportunities are provided for everyone to access electronic technologies, regardless of gender, race, religion, culture, ethnic group, physical ability or mental ability.

6. Special Needs

The school will ensure that children with Special Educational Needs are made aware of the risks and dangers of using ICT, within their understanding and abilities.

7. Managing School Network Access

7.1. The school will maintain one network systems.

7.2. The Business Manager (Mr. John Barker) will be responsible for the safe keeping of all associated administration usernames and passwords.

7.3. The Computing Leader (Mr. Michael Sheerin) will be responsible for the safe keeping of all associated curriculum administration usernames and passwords.

7.4. The network will be protected by antivirus software.

7.4.1. 'Datacable' are responsible for providing and updating this for the school network.

7.5. Access to the admin data will be restricted to senior management and office staff.

7.5.1. Levels of access to the admin data will be protected through unique usernames and passwords.

7.6. Access to the network is available to all teaching staff and pupils.

7.6.1. All staff access to the network is obtained with individual usernames and unique passwords. Staff will have access to a shared areas as follows:

7.6.1.1. Resources – Staff only read write access.

7.6.1.2. Exercises – Staff read and write access, Pupils read only access.

7.6.2. Staff will be able to access all pupil file space. *Staff must not allow pupils access to a computer which they have logged on to.*

7.6.3. Staff will have access to all pupil usernames and passwords.

7.6.4. All pupils from Y1 to Y6 will have their own username and file space.

7.6.5. Foundation stage will use a group username and password.

7.6.6. Children are allowed access to computer equipment at indoor playtimes and lunchtimes but may only access the websites on the school dashboard. Aimless browsing is not allowed.

7.6.7. Children will not be allowed to work in the IT Suite without staff supervision.

7.7. Visitors may be granted appropriate level of access to the network, (with permission from the Head teacher) through the use of visitors' usernames and passwords.

7.8. Contracted I.T. technicians may be given full access to the network, at the discretion of the Head teacher. All username and passwords used by I.T. technician must be declared to the Head teacher.

7.9. Staff should immediately report to the Headteacher, Business Manager and/or Computing Leader when they suspect there has been a breach of the Acceptable use policy or when passwords are, or are suspected of, having been lost, stolen, or disclosed.

8. <u>Managing Internet Access</u>

8.1. The Internet Service Provider for the school will be Schools Broadband.

8.2. Statutory UK ISP monitoring laws insist that Schools Broadband record all Internet usage.

8.2.1. Inappropriate use notifications will be provided by Schools Broadband filtering service and the Computing Leader will monitor these and forward to Head teacher and /or Safeguarding lead as appropriate.

8.2.2. The SWGFL Filtering test will also be used at the start of every term to monitor and ensure our connection filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse, the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online and the Adult Content Filter blocking access to pornography websites.

8.3. There are four school WiFi networks, which are password protected known only to the Computing Leader, Network technician, Business manager, Teaching Staff and Head teacher.

8.3.1. WL – Apple: for school iPads.

8.3.2. WL – Chromebook: for all school pupil Chromebooks.

8.3.3. WL – School: for all classroom PCs and teacher laptops.

8.3.4. WL – Guest: for staff mobile phones and visiting guests in need of internet access.

8.4. Staff must adhere to the school's "Acceptable Use Policy". (see appendix D)

8.4.1. Staff will exercise caution when surfing unfamiliar or untrusted websites

8.4.2. Staff will be specific in the use of words when using search engines

8.4.3. Staff will upload or download materials within the confines of copyright law.

8.4.4. Staff will always log out or lock a computer when not in use

8.5. Pupils must adhere to the school's "Internet / Online Code" when accessing the internet in school. (See appendixes A and B)

8.6. Pupils may only access the internet using school's electronic devices.

8.7. Pupils are not allowed to bring their own internet enabled electronic devices on to the school premises with the exception of mobile phones. These will be handed in before morning registration and stored in the main school office.

9. Managing Access to E-mail

9.1. **All incoming e-mail accessed using school computers should be treated as suspicious and attachments not opened unless the author is known.**

9.2. Staff will have access to e-mail through their Gmail account provided by the school Business Manager and Computing Leader.

9.2.1. Staff Gmail accounts are for school related use and can be used for private purposes in accordance with "Safer working practice."

9.2.2. Staff may access a private e-mail account on school premises in accordance with "Safer Working Practice". Staff must follow the school's "E-safety Guidance for Staff" when doing so.

9.2.3. Staff should inform the Head teacher if they receive offensive e-mail.

9.2.4 **Staff shall not:**

- Send messages using another user's accounts unless appropriately authorised to do so e.g. "sent on behalf of".
- Forward an e-mail from an address or person not recognised.
- Use language which might cause offence or be seen as abusive or discriminatory,
- Send or forward jokes, chain letters or other offensive or inappropriate content.
- Send files or documents from a computer that does not have up to date anti-virus and malware protection.
- Give out personal information or confidential information unless appropriately authorised to do so.
- Use a work-related email address to conduct personal business activities.

9.3. Pupils in KS2 will only be given access to global e-mail in conjunction with a computing project through a Gmail account created and managed by the school Computing Leader.

9.3.1. Pupils with be given clear guidance on how this email account can be used as part of the learning project.

9.3.2. Each class will be given a class Gmail account which is managed by the class teacher.

9.3.3. Pupils are not allowed to access a private e-mail account on school premises unless as part of a learning project and in the company of a member of staff.

9.3.4. Foundation and KS1 pupils will not be allowed access to global e-mail on school premises.

10. Managing Other Technologies

10.1. Published Content and the School Website

10.1.1. Staff or pupil personal information will not be published on the school website. The contact details given online should be the school office, class email or Head teacher.

10.1.2. The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

10.1.3. All material published on the school website must be the author's own work. If material from other sources is included credit should be given to the original author, stating clearly the source of such work and must not break copyright laws.

10.1.4. Pupils 'full' names will not be used anywhere on the school website, including image file names.

10.1.5. We will inform parents of our intention to use images of pupils on the school website, children can be excluded from this at the request of their parents or carers.

10.2. Social Networking and Personal Publishing

10.2.1. Pupils will not be allowed to access social networking sites, instant messaging sites or chat rooms, on school premises, unless permission is given by a teacher and used in a controlled environment as part of a learning project.

10.2.2. Pupils will not be allowed access to YouTube or similar video hosting websites on school premises, unless permission is given by a teacher and used in a controlled environment as part of a learning project.

10.2.3. As part of e-safety teaching and learning, pupils will be taught never to give out personal details of any kind which may identify them, their friends or their location. Pupils will be taught to always use nicknames and avatars and use only moderated, child friendly, age appropriate, social networking sites. Pupils will also be taught what is and is not suitable behaviour when communicating with others online.

10.2.4. Members of staff must not access social networking sites during normal timetabled hours. Staff may access personal social media and personal email during lunchtime. This can be done using the WL-Guest WiFi in the staff room, office, or classroom as long as there is no pupils present.

10.2.5. Members of staff must not accept pupils or parents, past or present as “friends” on social networking sites unless they are an actual relative.

10.3. IWB and YouTube

10.3.1. Staff must not stream live video from YouTube or similar video sharing websites in class on the IWB. Staff must capture and download the video beforehand or use a safe streaming service such as SafeshareTV or SafeYoutube.com

10.3.2. Live streaming from YouTube is permitted in Yr6 with ‘Restriction Mode ON’ and only after associated e-safety teaching has been completed.

10.3.3. Pupils are not permitted to access ‘YouTube’ or similar video sharing websites. These are blocked by the school Internet provider for pupil’s accounts.

10.4. Webcam Use

10.4.1. Laptop Webcams are not to be used by pupils unless permission is given by a teacher in a controlled environment as part of a learning project.

10.5. Mobile Phones

10.5.1. Staff use of mobile phone is governed by “Safer Working Practice” policy.

10.5.2. Pupils are not allowed to use mobile phones, or technologies built in to a mobile phone (e.g. camera), on school premises or during school activities off site.

10.6. Digital Cameras and Flip-Camcorders.

10.6.1. Staff and pupils may only use digital cameras and Flip-camcorders belonging to the school, as part of the curriculum project. These devices cannot be removed from the school premises unless permission by the Head teacher has been given.

10.6.2. Images and video taken of children must be downloaded from the device and saved in the designated folder (“Photos” or “Video clips”) on the school curriculum network. The device memory must then be deleted immediately afterwards.

10.6.3. Digital copies of images or video of staff or pupils must not be e-mailed or given to anyone without permission from the Head teacher.

10.6.4. Pupils are not allowed to use personal digital cameras or camcorders on the school premises.

10.6.5. If sanctioned by the Head teacher, pupils will be allowed to use personal digital cameras and camcorders on a school activity off the premises. Appropriate guidance will be given to the pupils.

10.7. Laptops, iPads and Chromebooks

10.7.1. When on the school premises, pupils may only use laptops, iPads and Chromebooks provided by the school. They are not allowed to bring personal devices on to school premises unless permission is given by a teacher and used in a controlled environment as part of a learning project.

10.7.2. Staff laptops, iPads and Chromebooks purchased by the school can be used for private purposes in accordance with “Safer Working Practice”. Staff laptops and iPads remain the property of the school and are open to scrutiny by senior management, contracted technicians and the Computing Leader. They must be password protected and any maintenance work required must be only done by “Datacable” the school’s curriculum ICT technician Service Company.

10.7.2.1. Staff laptops are encrypted using Bitlocker for additional security

10.7.3. Staff are not allowed to use personal laptops or iPads in school unless permitted by the Headteacher.

10.7.4. Staff are not allowed to install apps on to school iPads. This can only be done by the Network technician (Datacable) unless the teacher has been trained in the correct procedure and been given permission by the Headteacher.

10.8. External Hard-drives

10.8.1. Staff are not permitted to use external hard-drives to back up their files and resources. All back up and resources are to be sent to the cloud storage provided by the teachers Gmail account.

10.9. Emerging Technologies

10.9.1. Technologies not specifically covered by this policy can only be used on school premises at the discretion of the Head teacher.

11. Authorising Access

11.1. All staff must read “Acceptable Use - E-safety guidance for staff” before using any school ICT resource (see appendix D.)

11.2. Supply staff will be granted access to the curriculum network, with a generic username and password, they must read the “the “E-safety guidance for supply staff” before using any school ICT resource. (See appendix E.)

11.3. Visitors, who need to use ICT resources, must read the “E-safety guidance for visitors” information before being allowed to access the curriculum network or the internet. (See appendix F.)

12. Protecting Personal Data

12.1. All members of staff handling personal data and / or sensitive personal data, whether paper based or electronic, must adhere to the data protection principles within the Data Protection Act.

12.2. Every member of staff must take all reasonable steps to securely protect all data concerning pupils and others.

12.3. All school computer systems must be password and virus protected.

12.4. All staff laptops and staff iPads must be password protected.

12.5. Any data taken off the school premises should be kept to a minimum and if no longer required, deleted or destroyed in an appropriate manner, or returned to school for destruction.

12.6. All printed copies of personal data must be shredded before disposal as waste material

12.7. Hard disks from computers must be erased before machines are recycled or disposed of. Hard disks that have contained sensitive data (such as those from the admin network) should be destroyed.

12.8. Staff must take all reasonable care when using, storing and transporting memory devices sticks containing school data.

12.9. When working with personal or confidential data computer screens should be positioned where they are not easily visible from outside the immediate work area or by an unauthorized person.

13. Assessing Risks

13.1. The school will take all reasonable precautions to prevent access to inappropriate material.

13.2. The Computing Leader will continually monitor IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

14. Handling E-Safety Complaints

14.1. Complaints of pupil ICT/Internet misuse will be dealt with by a senior member of staff, who will decide if any sanctions are to be imposed and whether parents will be informed

14.2. Any complaint about staff misuse must be referred to the Head teacher, who will decide if any sanctions are to be imposed.

14.3. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

14.4. Any complaint about illegal misuse must be referred to the Head teacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by the Local Authority.

14.5. All employees and parents will be informed of the complaint's procedure.

14.6. Sanctions for minor incidents for pupils could include
- having network or internet access denied for a specified period

14.7. Sanctions for staff, could include
- receiving a verbal warning, of which a record is kept
- receiving a formal written warning
- formal disciplinary action being taken against an employee

14.8. Staff should note that copies of illegal material they find should not be sent / forwarded to anyone else, even as evidence, as this could also be seen an committing an illegal act.

14.8.1. Staff should not e-mail copies of illegal material to the Head teacher, E-Safety Leader, or Child Protection Coordinator as receiving such material could also be seen as the committing of an illegal act on their part.

15. Communicating Policy

15.1. Pupils

15.1.1. E-Safety rules and codes will be posted in all rooms where computers are used and discussed with pupils regularly.

15.1.2. A programme of training in E-safety is undertaken with all pupils using materials from CEOP and other internet safety organisation.

15.1.3. E-Safety training will be embedded within the computing curriculum and the Personal Social and Health Education (PSHE) curriculum.

15.1.4. The school website will contain e-safety information containing age appropriate resources and links for pupils to find out more. (Class Page – E-Safety)

15.2. Staff

15.2.1. All staff will be given access to the school E-Safety Policy and its importance explained.

15.2.2. Any training needs requested will be addressed. This includes annual updates on the use of CPOMs reporting/recording system.

15.2.3. All staff will be given the "Acceptable use Policy - E-safety guidance for Staff" document to read.

15.2.4. All supply staff will be given the "E-safety guidance for supply staff" (Appendix E) to read.

15.2.5. All visitors needing to use the ICT resources will be given the "E-safety guidance for visitors" (Appendix F)

15.3. Parents' and Carers'

15.3.1. Parents and Carers attention will be drawn to the School E-Safety Policy in newsletters and on the school website.

15.3.2. The school will maintain a list of e-safety resources for parents / carers on the school website. (Parents Page E-Safety)

16. Policy Approval and Review

16.1. This policy will be reviewed annually.

16.2. A full copy of this policy will be made available to all teaching staff, support staff and support staff.

16.3. A copy will also be available on the school website.

White Laith Primary School

E-safety

Using the Internet

Online Code

I will only use the Internet when I have permission.

I will never give out personal information on the Internet.

I will only use 'Swiggle' or 'Kiddle' to find information and pictures.

I will use only copyright free images when creating work to be printed out or published.

We will keep passwords secret

I will tell a teacher if anything I come across online make me worried or feel uncomfortable.

Digital Research Rules

1. Is the website is trustworthy? Check: Who is the author? Who does the author write for? Is it a reliable organization?

2. Go and look at other sites to compare.

3. Avoid clicking on adverts.

4. Always put information you use in to your own words. Never copy information from a website.

Appendix C

WHITE LAITH PRIMARY SCHOOL

ACCEPTABLE USE POLICY

Acceptable use of the school's ICT facilities and the internet: agreement for staff

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, extremist, 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 understand that I may use 4G/5G to access personal social media and personal email during lunchtime or out of timetabled teaching hours -this can be done in the staff room, office, or classroom as long as there are no pupils present. I will not use this to 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).

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) and ICT 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.

In line with school whistleblowing policies and KCSIE I will alert the Headteacher if I believe that any colleagues are in breach of this guidance. I will alert the Chair of Governors if I believe the Headteacher to be in breach of this guidance.

Appendix D

WHITE LAITH PRIMARY SCHOOL

E-safety guidance for – Supply Staff

This E-safety guidance is to ensure that any visitor is fully aware of their responsibilities. Once read the visitor may have access to and use the school ICT equipment.

- Only use of the school's ICT systems (including; hardware, software, email, Internet) and any related technologies for professional purposes.
- Do not connect any personal digital device, to any school computer system unless permission has been given by the Head teacher.
- Do not disclose any usernames or passwords provided by the school.
- Do not allow anyone else to use a computer when logged on using a username allocated by the school.
- Ask permission from the Head teacher before taking photographs of any kind.
- Never email or distributed outside the school digital copies of images of pupils and / or staff without permission from the Head teacher.
- If working with pupils, ensure they follow the school Internet Code.
- Take all reasonable steps to ensure that any school data given access to is used appropriately and remains confidential.
- Report any accidental misuse of school IT, or accidental access to inappropriate material, to the Head teacher.
- Report any incidents of concern regarding children's safe use of IT to the Head teacher.
- Do not use own internet enable device when pupils are present.
- Do not use YouTube, or similar websites, live, when pupils are present.
- Do not use social media or personal email accounts when pupils are present.
- Do not browse, download, upload or distribute any material that could be considered offensive, pornographic, obscene, extremist, illegal or discriminatory when using own internet enable device.
- Do not pass on personal e-mail address to pupils.
- Ask permission from the head teacher before taking copies of school software, data or documents from the school's computer systems off the premises.

Failure to comply with this E-safety guidance may result in sanctions being imposed, formal disciplinary action being taken or illegal use being reported to the appropriate authority.

Appendix E

WHITE LAITH PRIMARY SCHOOL

E-safety guidance for - Visitors

This E-safety guidance is to ensure that any visitor is fully aware of their responsibilities. Once read the visitor may have access to and use the school ICT equipment.

- Only use the school's ICT systems (including; hardware, software, email, Internet) and any related technologies for professional purposes.
- Not to connect any personal digital device, to any school computer system unless permission has been given by the Head teacher.
- Do not disclose any usernames or passwords provided by the school.
- Do not allow anyone else to use a computer when logged on using a username allocated by the school.
- Ask permission from the Head teacher before taking photographs of any kind.
- Never email or distributed outside the school digital copies of images of pupils and / or staff without permission form the Head teacher.
- If working with pupils, ensure they follow the school Internet Code.
- Take all reasonable steps to ensure that any school data given access to is used appropriately and remains confidential.
- Report any accidental misuse of school IT, or accidental access to inappropriate material, to the Head teacher.
- Report any incidents of concern regarding children's safe use of IT to the Head teacher.
- Do not use own internet enable device when pupils are present.
- Do not use YouTube, or similar video sharing websites, live, when pupils are present.
- Do not use social media or personal email accounts when pupils are present.
- Do not browse, download, upload or distribute any material that could be considered offensive, pornographic, obscene, illegal or discriminatory when using own internet enable device.
- Do not pass on personal e-mail address to pupils.
- Ask permission from the Head teacher before taking copies of school software, data or documents from the school's computer systems off the premises.

Failure to comply with this E-safety guidance may result in sanctions being imposed, formal disciplinary action being taken or illegal use being reported to the appropriate authority.

Appendix F

Facebook - guidance for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Don't accept friend requests from pupils on social media
2. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
3. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
4. Check your privacy settings regularly
5. Be careful about tagging other staff members in images or posts
6. Don't share anything publicly that you wouldn't be just as happy showing your pupils
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