Online Safety Policy

June 2021 – June 2022

Approved by Governing Body on / /

Contents:

At Headley Park Primary School, we understand that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

1.1. This policy has due regard to the following legislation and guidance, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000

- **Regulation of Investigatory Powers Act 2000**
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2021) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- UK Council for Child Internet Safety 'Education for a Connected World'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

1.2. This policy will be used in conjunction with the following school policies and procedures:

- CST Safeguarding and Child Protection Policy
- CST Anti-Bullying Policy
- CST Data Protection Policy
- CST Employment Manual
- Staff Code of Conduct policy
- Pupil Mobile Phone Policy

2. Use of the internet

1.3. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

1.4. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

1.5. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information

- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

1.6. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such, as a priority.

1.7. The governing body and the lead safeguarding governor are responsible for holding the school to account to ensure this policy is reviewed on an annual basis, staff undergo safeguarding and child protection training which includes online safety training and that there are appropriate filtering and monitoring systems in place to safeguard pupils.

1.8. The schools Designated Safeguarding Lead (DSL), alongside the Online Safety Lead teacher, act as the Online Safety Leaders and are responsible for ensuring the day-to-day Online Safety in school and managing any issues that may arise.

1.9. The headteacher is responsible for ensuring that the Online Safety Leaders and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

1.10. The Online Safety Leaders will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

1.11. The headteacher will ensure there is a system in place which monitors and supports the Online Safety Leaders, whose role is to carry out the monitoring of Online Safety in the school, keeping in mind data protection requirements.

1.12. The Online Safety Leaders will regularly monitor the provision of Online Safety in the school and will provide feedback to the headteacher.

1.13. A log of submitted Online Safety reports and incidents will be regularly updated using the schools CPOMs system.

1.14. The headteacher will maintain a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

1.15. The Online Safety leaders will ensure that all members of staff are aware of the procedure when reporting Online Safety incidents.

1.16. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

1.17. The safeguarding governor will challenge the effectiveness of the Online Safety provision and current issues, as well review incident logs, as part of regular safeguarding meetings and through the 'At a glance document' in line with the school's duty of care.

1.18. The Online Safety Leaders in conjunction with the Safeguarding governor will evaluate and review this Online Safety Policy and procedures on a regular basis, taking into account new legislation, government guidance, previously reported incidents, the latest developments in ICT and the feedback from staff/pupils.

1.19. Teachers are responsible for ensuring that Online Safety issues are embedded in the curriculum and safe internet access is promoted at all times.

1.20. CST IT technicians are responsible for providing technical support implementing, maintaining and updating appropriate security measures, filtering and monitoring systems.

1.21. All staff are responsible for ensuring they are up-to-date with current Online Safety issues, and this Online Safety Policy.

1.22. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement (see appendix) which they must sign and return to the headteacher.

1.23. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

1.24. The Online Safety Leaders are responsible for communicating with parents regularly and updating them on current Online Safety issues and control measures.

1.25. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. Online Safety education

1.26. Educating pupils:

- Online Safety is taught across the curriculum, however, it is particularly addressed in PSHE, RSE and computing as well as through specific events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.
- Pupils will be made aware of the safe use of new technology both inside and outside of the school.
- Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.
- The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

o How to evaluate what they see online
o How to recognise techniques used for persuasion
o Acceptable and unacceptable online behaviour
o How to identify online risks
o How and when to seek support

- Online safety teaching is always appropriate to pupils' ages and developmental stages.
- Pupils will be taught about the importance of Online Safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE and RSE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

1.27. Educating staff:

- All staff will undergo Online Safety training on a regular basis to ensure they are aware of current Online Safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo Online Safety training as part of their induction programme, ensuring they fully understand this Online Safety Policy.
- The Online Safety Lead will act as the first point of contact for staff requiring Online Safety advice.

1.28. Educating parents:

- Online Safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Courses and presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any Online Safety related concerns.

5. Online Safety control measures

1.29. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.
- A record will be kept of all pupils who have been granted internet access.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The CST ICT technician will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Technical security features, such as anti-virus software, are kept up to date and managed by CST ICT technician.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.
- Master users' passwords will be available to the headteacher and Online Safety Lead for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the Online Safety lead for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Users are required to lock access to devices and systems when they are not in use.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in section 7.4 of this policy.

1.30. Email:

- Staff will be given approved email accounts to be used for school communications. The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Staff members are aware that their email messages are **not** monitored.

- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

1.31. Social networking:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are allowed to access and post to the school twitter account for the purposes of celebrating events in school and promoting the school.

1.32. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential

information regarding the school, or any information that may affect its reputability.

1.33. Mobile devices

- Examples of mobile devices include (but is not limited to) items such as mobile phones, tablets and handheld computers.
- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices.
- Mobile devices are not permitted to be used during school hours by pupils
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the Online Safety Lead when using these on the school premises.
- Staff are permitted to use their mobile devices for taking photographs for the purpose of sharing on the school Twitter account, for classroom displays or as evidence of a child's learning. These photos must be deleted from personal devices within 48 hours (Please refer to the CST acceptable use policy).
- The sending of inappropriate messages or images from school mobile devices is prohibited.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

1.34. Network security:

- Network profiles for each staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords should be stored using non-reversible encryption.

1.35. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the technical support team at CST.
- The technical support team will ensure that the filtering of websites and downloads is up-to-date and monitored.

6. Responding to specific online safety concerns

1.36. Cyber bullying

- For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.
- The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

1.37. Online sexual violence and sexual harassment between children (peer-on-peer abuse)

- The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

- Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the CST Child Protection and Safeguarding Policy.

1.38. Upskirting

- Upskirting is not tolerated by the school.
- Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the CST Child Protection and Safeguarding Policy.

1.39. Youth produced sexual imagery (sexting)

- All concerns regarding sexting are reported to the DSL and will be dealt with in line with the CST Child Protection and Safeguarding Policy

1.40. Online abuse and exploitation

- Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the CST Child Protection and Safeguarding Policy.

1.41. Online hate

- The school does not tolerate online hate content directed towards or posted by members of the school community.
- Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved (eg Staff Code of Conduct, CST Anti-Bullying Policy, CST Child Protection and Safeguarding Policy etc.)

1.42. Online radicalisation and extremism

- The school's filtering system protects pupils and staff from viewing extremist content.

- Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the CST Child Protection and Safeguarding Policy and the Prevent Duty.

7. Reporting misuse

1.43. Inappropriate behaviour is defined in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

1.44. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to Online Safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

1.45. Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, will be reported to the DSL and be dealt with in accordance with our Child Protection and Safeguarding Policy.

1.46. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the CST employment manual and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

1.47. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

8. Monitoring and review

1.48. The safeguarding governor and Online Safeguarding Lead will review this Online Safety Policy on a regular basis, taking into account the school's Online Safety calendar, the latest developments in ICT and the feedback from staff/pupils.

1.49. Reviews will be shared with the wider governing body and any changes made to this policy will be communicated to all members of staff.

1.50. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Appendices

Student Acceptable Use Agreement – Information for Parents/ Carers

School Policy:

- Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

For child's personal safety they will agree to the following:

- I understand that the school will monitor my use of the systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will be aware of "stranger danger", when I am communicating online;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc);
- I will not arrange to meet people off-line that I have communicated with online;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not use the school systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones / USB devices etc) in school without prior permission;
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will immediately report any damage or faults involving equipment or software, however this may have happened;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings;
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not try to download copies (including music and videos);
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information);
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

- ***Please complete the sections below and on the following page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.***

Student Acceptable Use Agreement

This is how we stay safe when we use computers:

- **I will ask a teacher or suitable adult if I want to use the computers;**
- **I will only use activities that a teacher or suitable adult has told or allowed me to use;**
- **I will take care of the computer and other equipment;**
- **I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong;**
- **I will tell a teacher or suitable adult if I see something that upsets me on the screen;**
- **I know that if I break the rules I might not be allowed to use a computer.**

Signed (child): ……

Signed (parent): ……

Date: ……

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras, iPads and phones to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website, on the school twitter account and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

Digital / Video Images Permission Form

Parent / Carers Name	
Student Name	

As the parent / carer of the above student, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Please tick each section you agree to permit

- For use within school e.g assessment, displays, newsletter and private youtube channels (not for the general public) ☐
- The school website, HPPS Twitter account and general media (available to the public) ☐