The Hawthorns Primary School

‘All in one’
e-Safety Policy

Agreed and Adopted by the Governing Body on: 27 June 2023

Signed : J Shepherd

The policy will be formally reviewed on: June 2026

Wokingham

'All in One' e-Safety Policy

Contents:

1 Roles and Responsibilities

1.1 Governors

Governors are responsible for the approval of the e-Safety Policy (including Use Agreements), ensuring that it is implemented and reviewing its effectiveness. To assist in fulfilling this responsibility The Governing Body of The Hawthorns Primary School has an appointed a IT Governor. The IT Governor will undertake the following regular activities:

- Meetings with the e-Safety Co-ordinator.
- Monitoring of e-Safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school e-Safety matters.

1.2 Headteacher

The Headteacher is responsible for ensuring the safety, including e-Safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the Keeping Children Safe in Education statutory guidance). The day to day responsibility for e-Safety may be delegated to the e-Safety Co-ordinator or another appropriate member of staff. However, the Headteacher will ensure the following:

- Staff with e-Safety responsibilities receive suitable and regular training enabling them to carry out their e-Safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives an annual monitoring report.
- There is a clear procedure to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- All members of staff, student teachers and volunteers adhere to the IT Code of Conduct and Safeguarding policy.

1.3 e-Safety Co-ordinator

The e-Safety Co-ordinator has day to day responsibility for e-Safety issues and takes a leading role in establishing and reviewing the school e-Safety Policy and associated documents. The e-Safety Co-ordinator will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide materials and advice for integrating e-Safety within schemes of work and check that e-Safety is taught on a regular basis.
- Liaise with the school's Designated Safeguarding Lead.
- Liaise with the Local Authority.
- Liaise with the school's technical and technical support staff.
- Ensure that e-Safety incidents are reported and logged and used to inform future e-Safety developments.
- Report to the governors and meet with them as required.
- Report to the SLT when required.

The e-Safety Co-ordinator is the Headteacher.

1.4 IT Technician

The IT Technician in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.

- The school meets the e-Safety technical requirements outlined in any relevant Local Authority e-Safety policy/guidance e.g. LA model policy/guidelines.
- Users may only access the school's network(s) through a properly enforced password protection policy, in which passwords are recommended to be changed each term, as per the IT Code of Conduct (Appendix 6a)
- The school's internet filtering system is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- e-Safety technical information is kept up to date, applied as necessary and passed on to others where relevant.
- Use of the network, online learning provision and web use is regularly monitored and any misuse/attempted misuse reported to the e-Safety Co-ordinator. Appropriate steps are taken to protect personal information and secure data on all devices and removable media in line with our General Data Protection Regulation Policy (GDPR)
- Provide secure access to the school network from home where necessary using remote desktop or equivalent technologies.

The school support provider is SoftEgg.

1.5 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current e-Safety matters and the school e-Safety Policy and practices.
- They have read and understood the school's IT Code of Conduct and signed to indicate agreement.
- They report any suspected misuse or problem to the e-Safety Co-ordinator for investigation and action.
- Digital communications with pupils (Learning Platform/ Google meet) should be on a professional level and only carried out using approved school systems.
- e-Safety issues are embedded in all aspects of the curriculum and other school activities.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-Safety issues related to the use of mobile phones, cameras and teaching devices and that they monitor their use and implement school policies with regard to these e.g. Chrome books.
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.
- Student teachers and volunteers to understand and adhere to this e-safety policy and sign the IT Code of Conduct.
- Pupils understand and follow the school's e-Safety guidance. Staff follow the DfE Teaching Online Safety Guidance.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.

1.6 Designated Safeguarding Lead (DSL) /Child Protection Officer (CPO)

The DSL/CPO should be trained in e-Safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

The Designated Safeguard leads are the Headteacher and the Deputy Headteacher.

1.7 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk. SLT should be informed where school policies may require updating.

[See *'Appendix 1 – School and the Data Protection Act'* for further information]

The Designated Data Controller is the School Business Manager.

2 Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually, or sooner if necessary.
- The school will audit IT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of the school devices will sign the appropriate agreements. This includes all staff and volunteers who use a school device/Remote Desktop Services or are provided with data on an electronic device or cloud services. All users will be expected to re-sign agreements if amendments have been made. This does not apply to pupil/parent Home School Agreements unless changes are significant.
- All BYOD users will be referred to the policy.

2.3 Reporting

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.
- e-Safety incidents, misuse of the internet/technology should be reported to the e-Safety Co-ordinator or in their absence a member of the Senior Leadership Team.
- All concerns reported will be recorded in the e-Safety Incident Log Book located in the Headteacher's tray.

  [See *'Appendix 2 – Course of action if inappropriate content is found'* for further information]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and Safeguarding Policy.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour.
- If an e-Safety allegation is made against a member of staff, the member will be subject to the Schools Disciplinary process and policy.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

3 Communications & Communication Technologies

3.1 Mobile phones and personal devices (including smartwatches, Bluetooth and digital wireless devices)

To ensure the safety and well-being of our pupils we ask all staff, volunteers, parents and pupils to adhere to the following:

- Pupils will not be allowed to bring mobile phones or personal devices to school unless prior arrangements are made with the school.
- Where mobile phones/personal devices are allowed in school, they may not be used during lessons or formal school time.
- The sending of abusive or inappropriate messages is forbidden.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
- Pupils are not allowed to bring personal devices, including tablets/laptops to school unless prior arrangements are made under the Bring Your Own Device Policy.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- The school has a strict no mobile phone policy where children are present throughout the school. (refer to the school's Safeguarding Policy). Staff, parent, volunteer and visitor mobile devices may normally be switched off where children are present. Mobile devices may be on silent during the times that children are not present e.g. staff room, office areas
- Mobile devices can only be used on a designated break away from the children unless cover has been arranged to enable the staff member to leave the class.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Parents, Volunteers in school and Staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they got to the office or the staff room to make a call.

Whilst we recognise that there may be emergency situations which necessitate the use of a mobile phone/device, in order to ensure the safety and welfare of children in our care; staff, parents, volunteers and visitors are to refrain from using their mobile phones and devices in school during school hours.

If you are found to be using your phone within the school premises you may be asked to finish the call and to take the call outside.

3.2 E-mail and messaging

- Pupils and Staff will be informed that the use of school e-mail or messaging accounts will be monitored.
- Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- Staff should use bcc as best practice wherever possible.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils may only use approved e-mail or message accounts on the school system.
- Pupils should immediately tell a staff member if they receive an offensive e-mail or message.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.

- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.
- Information of a sensitive nature should only be sent by the internal school e-mail system.

3.3 Social networking

For the purpose of this policy, social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, Instagram, blogs, chat rooms, Whatsapp, YouTube, Messenger, Google Meet, Microsoft Teams etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within a school online learning provision is both acceptable and to be encouraged.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- The school community staff, parents and pupils are reminded of best practice with regards to online use and social media networking.
- School staff should never be 'friends' with the children at the school or past pupils up to the age of 18.
- School has a 'Facebook' Site that is managed in line with our Safeguarding Policy and duty to Keeping Children Safe in Education.

[See *'Appendix 3 – Social Networking Guidance'* for further information]

3.4 Internet usage

- Pupils and Staff will be informed that internet access will be monitored.
- 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. The school cannot accept liability for the material accessed, or any consequences of internet access. The school will take appropriate measures to prevent a reoccurrence, including contacting the service provider.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's e-Safety Guidelines. These should be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a regular basis as per Item 2.3.

3.5 Remote Desktop Services (RDS)

3.5.1 Access

- RDS is provided to Staff and Student teachers as requested. Instructions are provided by the IT technician.
- RDS access is governed by the password guidelines stated in this policy.

3.5.2 Constraints

- RDS must not be used on public networks.
- Screens must be locked when the device using RDS is unattended.

- No other person should have access to RDS other than the person who requested access. e.g. family members on a shared home device.
- The user must not allow default access.

3.5.3 Considerations

- All users to be aware of sensitive data and our data protection policy
- All users to abide by the IT Code of Conduct
- All users to abide by the school's Safeguarding Policy
- All users to abide by the school's Code of Conduct
- Monitoring of usage will take place as per this policy for e-safety purposes.

3.5.4 Rules

- Access will be revoked if there is evidence of unacceptable/inappropriate use
- Access will be removed/disabled at the termination of an employee's contract or the completion of a student teacher placement.

3.6 Remote Learning

Refer to the schools Remote Learning Policy for occasions when face to face learning is not possible. The Remote Learning Policy works in conjunction with this policy.

3.7 Digital and video images/Audio Devices

To ensure the safety and well- being of our pupils we ask all staff, volunteers, parents and pupils to adhere to the following, this works in conjunction with section 3.1:

3.7.1 Parental permission

- The school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use could include the school website, online learning provision or social media (currently Facebook and Instagram); display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- If specific individual pupil photographs are to be used publicly, such as on the school website, in the prospectus or any other high profile publication, then a check should be made with individual parents for this additional use.
- Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

3.7.2 Storage and deletion

- All images of pupils will be securely stored in one central location.
- Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.

- Images may be retained for up to 5 years after a pupil has left the school and are then deleted in line with the GDPR Policy. An exception to this would be where parental consent has been granted for the imagery to be used in a significant school event or project.

3.7.3 Recording of images/audio

- All staff and pupils must sign the Acceptable Use Agreement and IT Code of Conduct.
- School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images/audio of others without their permission.
- Where images/audio are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online 'cloud' storage) care must be taken that the location of images of pupils is clearly understood and in line with ICO (Information Commission's Office) guidance.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Parents, volunteers in school should abide by the same rules as school staff as far as is reasonable, as per the Volunteers Policy.

  No images of pupils should be recorded

  -in toilets or wash areas

  -whilst pupils are getting changed

  -in the medical room

  The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g. how to wash hands). In this case the line manager must be informed before this activity is undertaken.

3.7.4 Use of staff personal devices

It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. Where a school wishes to vary from this, e.g. for off-site activities, the following should apply:

- It will be clearly understood under what circumstances it is permissible to use a personal device.
- Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies deleted.
- Audio devices e.g. Amazon Alexa, should be used in accordance with the schools Bring your own device and e-safety Policy.
- Staff personal devices should be passcode protected.

At The Hawthorns, staff and volunteers must seek the authorisation of the Headteacher prior to taking photographs/ videos of children and must only use school equipment unless given specific authorisation by the Headteacher. The use of cameras on mobile phones or any personal electrical device is forbidden. Downloading of images from school equipment is only for the purpose of the school. Downloading of images from school equipment for the school website must be with permission from the parent as per the school's Safeguarding Policy.

3.7.5 Parents taking photographs or video

Where the school chooses to allow the recording of images at 'public' events the following should apply:

- Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

3.7.6 Events/Activities involving multiple schools

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.
- Parents will be informed prior to an event, as per the school's policy that images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.
- Images of pupils must be stored securely for historical evidence and deleted when no longer required.
- The school will add a disclaimer to all letters addressed to parents/carers and pupils regarding assemblies and trips, highlighting the safeguarding concerns of digital and video images.

As per the school's Safeguarding Policy and Volunteers Policy there are many legitimate circumstances in which for employees and volunteers to photograph or film children in the course of their job. However, to ensure the safety of all children and to protect the adults concerned, any photographing or filming of children must be done using equipment provided by the school for that purpose. Personal cameras may only be used with permission from the Headteacher and mobile phone cameras must never be used for photographing children. If this permission has been granted, then once the images/audio are downloaded on to the school system they must be immediately deleted from the personal device. Evidence of this should be acknowledged by the e-safety co-ordinator or the Designated Safeguarding lead.

3.8 Learning Platform and/or website

- The school Learning Platform and/or website should include the school address, school e-mail and telephone number including any emergency contact details.
- The school Learning Platform and/or website should be used to provide information and guidance to parents concerning e-Safety policies and practice.
- Staff or pupils' home information should not be published.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.

4 Infrastructure and Security

4.1 Security

The school will be responsible for ensuring that the digital infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School IT technical staff may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets, should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the IT Technician.
- Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- The 'Administrator' passwords for the school IT system, used by the IT Technician are also available to the IT Subject Leader and are stored securely in school safe.

4.2 Passwords

All staff are provided with an individual password. Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the online learning provision and/or secure areas of the website.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- 'Strong' passwords should be used. No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- Once a device has been used, users must remember to log off so that others cannot access their information.
- All staff leaving a computer temporarily should lock the screen (Windows key + L).
- Passwords to the school network are changed every 90 days. Staff will be reminded to change their password by a prompt.
- In the event that a password becomes insecure then it should be changed immediately.

  [See *'Appendix 4 – Password guidance'* for further information]

4.3 Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

- Changes to network filtering should be approved by the IT Subject Leader and the IT Technician.
- Any filtering issues should be reported immediately to the ISP and/or SEGfL.

4.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an anti-virus product which is preferably administered centrally and automatically updated.
- The ant-virus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only dependable sources should be used.
- Staff should report to the IT Technician or e-Safety Co-ordinator if the removal of adware and malware is required.

4.5 School laptops/devices/Chromebook

- The use of school laptops/devices/Chromebooks must only be used for school purposes.
- School laptops/devices/Chromebooks and flash drives are likely to be taken out of school and may well contain sensitive data (see Section 3.6). School must encrypt laptops which are taken off site. School laptops/devices/Chromebooks must not have any social media or messaging apps on them. Apps downloaded must be for educational purposes only and be downloaded by IT leader or technician. This is to ensure age appropriate and safe apps.
- Passwords must not be shared or written down.

School devices must not be taken home unless approved by the IT technician. The following security measures should be taken with staff laptop/devices:

- All staff must sign a Device Loan Agreement if they wish to take a Laptop off site.
- Laptops/devices must be out of view and preferably locked away overnight or secured to prevent removal. Laptops/devices should never be left in a parked car, even in the boot.
- Screensavers should be set to lock after a maximum of 15 minutes.
- Laptops/devices should not normally be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

4.6 General Data Protection Regulation (GDPR)

See GDPR Policy for specific guidance in relation to the security of personal data.

- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- Sensitive data is any data which links a child's name to a particular item of information and/or the loss of which is liable to cause individuals damage and distress. Therefore, such data:
  - must be encrypted on laptops/devices, memory sticks, and any other removable media;
  - should only be e-mailed between staff on the school's e-mail system;
  - should be deleted from devices at the end of an academic year or earlier if no longer required.
- Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.
- There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.
- All users to acknowledge and adhere to Data Protection (GDPR) policy.
  [See *'Appendix 5 – Sensitive and Non-Sensitive Data'* for further information]

4.7 Electronic devices- search and deletion

Schools now have the power to search pupils for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices/mobile phones. Clear guidelines relating to this should be communicated to staff and parents if required. Such guidelines would include;

- Details of which items are banned under the school rules and may be searched for e.g. mobile phones without prior agreement.

- A list of staff members/roles authorised to examine and/or erase data on electronic devices e.g. class teacher
- Clear guidance as to what is, and is not, allowed when searching a pupil
- When data will be deleted or kept as evidence
- How incidents will be recorded

4.8 Loading/installing software

For the purpose of this policy, software relates to all programs, apps, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the IT Technician or IT Subject Leader, may load software onto the school system or individual computers.
- Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

4.9 Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of key school information is via a secure encrypted online backup system.
- No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The schools Rainbow Plan, contains information on the school's back up recovery plan that would take effect when severe disturbance to the school's IT infrastructure takes place.

5. e-Safety Education

5.1 Learning and teaching for pupils

- Pupils should be encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils should be taught to be critically aware of the materials/content they access on-line.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key e-Safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers should be displayed in all rooms. School provides workshops/assemblies for upper Key Stage 2 children annually.

5.2 Staff training

- Staff will be kept up to date through regular e-Safety training.
- Staff should always act as good role models in their use of IT, the internet and mobile devices.
- The staff handbook contains the e-Safety Policy and the DfE guidance for Teaching Online Safety.
- Staff should be aware of the schools Whistleblowing policy with regards to e-Safety and Safeguarding.

5.3 Parental support

The support of, and partnership with, parents should be encouraged. This is likely to include the following:

- Awareness of the school's policies regarding e-Safety and internet use. Practical demonstrations and training
- Advice and guidance on areas such as:
  - filtering systems
  - educational and leisure activities
  - suggestions for safe internet use at home
  - Online social media use
  - Invite parents to attend e-safety presentations
  - Provide parents with e-safety guidance on the school website.

Management of this policy

The policy should be reviewed every 3 years.

The Headteacher is the current e-Safety Co-ordinator and Mrs C Burgess is the e-Safety Assistant

Mrs Asmita Gore is the current IT Governor responsible for e-Safety.

Additional information:

This policy should be read in conjunction with

- Safeguarding Policy
- Prevent Policy
- Volunteers Policy
- Home School Agreements (Behaviour Management Policy)
- Code of Conduct and Personal Behaviour
- IT curriculum Policy
- Complaints Policy Staff Handbook
- Teachers' Standards (DfE, 2012)
- Inspecting Safeguarding-Ofsted
- Disciplinary Policy
- Bring Your Own Device Policy- Staff and Pupils
- Online and Social Media use
- Parental photo permission form in the Pupil Starter Information Pack
- General Data Protection and Regulation (GDPR)
- Department for Education Keeping Children Safe in Education guidance
- Teaching & Learning Policy
- Department for Education Teaching Online Safety in school
- Remote Learning Policy
- Whistleblowing Policy

Appendix 1 – School and the Data Protection Act

The Seventh Principle of the Data Protection Act (2018) states that:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

This means that schools must have appropriate security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.

The implications of this for the school will be the need to:

- Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear about who is responsible for ensuring information security.
- Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
- Respond to any breach of security swiftly and effectively.

Failure to comply with the Act could result in loss of reputation or even legal proceedings.

Further guidance may be found at www.ICO.gov.uk

Appendix 2 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the e-Safety Co-ordinator.
- The e-Safety Co-ordinator will then:
    - Log the incident and take any appropriate action.
    - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

Appendix 3a – Social networking guidelines Staff

Specific guidelines relating to staff use of social networking are best arrived at through discussion to both clarify and agree exactly what should be applicable. Aspects will also be applicable to those associated with the school, e.g. governors and parent helpers.

Specific guidelines relating to the schools use of Social Media are best arrived at through discussion to clarify and agree exactly what should be applicable. Currently the schools Facebook page and Instagram account are for the purposes of marketing and communicating to our community.

The following areas should be considered for inclusion:

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' on-line space.

Access to social networking sites

- Social networking sites should not be used or accessed during school working hours unless this is part of a classroom task or through the use of the online learning provision. All sites used as a learning resource should be previewed for their content and shown to the pupils in full screen to remove advertisements.
- Staff may not use school equipment to access social networking sites for personal use
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals using Staff Proxy to bypass filtering.

Posting of images and/or video clips

- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.
- Posting of images will be in accordance with our Safeguarding Policy.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Additional considerations

Thought should be given to what the implications of this policy will be for the different groupings within the staff employed at the school, e.g.

- Teacher
- Teaching assistant

- Other support staff, e.g. school's business manager, site manager, lunchtime supervisors, office staff, cleaners
- Outside agency staff, e.g. sports coaches, music tutors, etc.
- Volunteers, visitors, etc

Appendix 3b – Social networking guidelines

Online and social media use

The use of computers and social media has become an integral part of our lives. As parents and carers we accept that technology is part of modern civilisation, however we have a responsibility to teach and protect our children through our own behaviour and e-safety knowledge.

The school community is asked to promote the following behaviour:

To show common courtesy online;

- We ask permission before uploading photographs, videos or information about others online.
- We do not write or upload hurtful, rude or derogatory material. This is disrespectful, can upset, can cause distress, be an act of bullying or harassment.

To show common decency online;

- We do not post comments that can be considered as being prejudicial, intimidating or defamatory.
- We do not forward comments that exist online, such as emails, video, chat etc. Forwarding can make you liable.

To show common sense online WE THINK…..

  - before we 'click'
  - before we upload
  - before we download or forward
  - carefully about what information we share with others,
  - we check where it is saved
  - we check our privacy settings

- We make sure we understand changes in use of any sites or applications that we use
- We block harassing communications and report abuse

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

Social media has become a significant part of modern life. In the event that any member of staff, pupil or parent/carer is found to be posting libellous or inflammatory comments on any social media sites, they will be reported to the appropriate 'report abuse' section of the site.

In serious cases we will consider legal options to deal with misuse.

The whole school community is reminded of the CEOP report abuse process this can be found on our website.

Appendix 4 – Password guidance

- Passwords should have a minimum of 8 characters and include letters and numbers.
- Passwords must not be easily guessable by anyone and therefore should not include:
    - Names of family, friends, relations, pets etc.
    - Addresses or postcodes of same
    - Telephone numbers
    - Car registration numbers
    - Unadulterated whole words
- Try to use in a password:
    - A mixture of letters and numbers
    - Punctuation marks
    - At least 8 digits
- Possible ideas are
    - Choose a word which has "o" and """ in and substitute 0 (zero) and 1, e.g. sn0wt1me.
    - Use the initial letters of a familiar phrase, song title etc. and substitute as above.
    - Use a text message abbreviation, e.g. CUL8R

- Staff will be prompted to change passwords every 90 days on resources that contain personal or sensitive data (e.g. PC's, email, remote desktop,)

Appendix 5 – Sensitive & Non-sensitive data

Sensitive data will include:

- SEND records such as IEPs and Annual Review records
- Mark sheets and assessments
- Reports and Open Evening comments
- Personal data stored on the school's Management Information System, e.g. SIMS
- Photographic or video material
- Name, address and contact information

Non-sensitive data thus includes:

- General teaching plans
- Curriculum materials
- General correspondence of a non-personal nature

Appendix 6
Device Loan Agreement

This Agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school. It should be read in conjunction with the school's e-Safety Policy. All recipients and users of these devices should read and sign the agreement.

1. The laptop/device remains the property of the school and is only for the use of the member of staff it is issued to.
2. The laptop/device should be stored and transported securely. Special care must be taken to protect the equipment and any removable devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage/loss.
3. Staff should understand the limitations of the school's insurance cover. Insurance excludes accidental damage and theft from a car. If the laptop/device is stolen from an unattended car, you will be responsible for its replacement. The equipment does not carry separate insurance other than that already pertained by the school.
4. Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.
5. Only software licensed by the school, authorised by the Headteacher and installed by the school's IT Technician may be used. No personal software should be loaded. Users should not attempt to make changes to the software and settings that might adversely affect its use.
6. Anti-virus software is installed and must be updated in compliance with instructions.
7. Should any faults occur, notify the IT Technician as soon as possible. Under no circumstances should staff attempt to fix suspected hardware faults.
8. Any connection charges incurred by staff accessing the internet from home are not chargeable to the school.

Laptop make:	Model:
Serial no:	
Headteacher Authorisation:	Date:
Member of Staff:	
Received by:	Date:

6a

The Hawthorns Primary School

IT Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's e-Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or a printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. e-Safety Co-ordinator, DSL and/or SLT member.
- I am aware that my password will be required to be changed every 90 days.
- I am aware that this code of conduct applies to working remotely.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	