Snape Wood Primary and Nursery School

Excellence for All

‘To provide excellence for all within a happy, safe, and stimulating learning environment’

E-SAFETY POLICY

Name of School: SNAPE WOOD PRIMARY AND NURSERY SCHOOL	
Policy Reviewed Date: Spring 2023	
Date of next review: Spring 2024	**Date adopted by the Governing Body:**
Annually	Spring 2020
Signed **Shewley Choudhury** **(Headteacher)** **Signed** **Danny Hall** **(Chair of Governing Body)**	

E-SAFETY POLICY

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Snape Wood Primary and Nursery School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Snape Wood Primary and Nursery School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content
- Social media and the use of such apps to promote bullying/racism/sexual harassment/ extremist views

Contact

- Grooming (sexual exploitation, radicalisation etc)
- Online-bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling body image) • sexting
- Copyright (little care or consideration for intellectual property and ownership ¡V such as music and film)

Scope

This policy applies to all members of the Snape Wood Primary and Nursery School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and use of electronic devices and the deletion of data. Snape Wood Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour that take place out of school.

Role	Key Responsibilities
Everyone	• To ensure that data is adequately protected under new GDPR guidelines as of 25/5/2018. • If using a laptop/ desktop, to lock their account if they leave the screen/room throughout the day (CTRL + L). • Keep memory sticks, internal and external storage devices etc. secure with a bitlocker password.
Head teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Coordinator
	□ To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager □ To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety □ To ensure school website includes relevant information. □ ensure that the school follows all current e-Safety advice to keep the children and staff safe □ (along with the governors) approve the E-Safety Policy and review the effectiveness of the policy. □ supports the school in encouraging parents and the wider community to become engaged in e-Safety activities.

Role	Key Responsibilities
Computing coordinator/Head teacher	• takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school's e-Safety policies • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-Safety education is embedded across the curriculum • liaises with school ICT technical staff • ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • ensures that an e-Safety incident log is kept up to date • facilitates training and advice for all staff • Liaise with LA and relevant agencies • Liaises with the Local Authority and relevant agencies • Is regularly updated in e-Safety issues and legislation, and is aware of the potential for serious child protection issues that can arise from: 1. The sharing of personal data 2. Access to illegal / inappropriate materials 3. Inappropriate on-line contact with adults / strangers 4. Potential or actual incidents of grooming 5. Cyber-bullying and use of social media.
Computing Coordinator	• oversee the delivery of the e-Safety element of the Computing curriculum • To ensure that the computing curriculum is relevant and kept up to date.
LA Network support technician	• ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • ensure the security of the school ICT system • ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • ensure that the school's policy on web filtering is applied and updated on a regular basis • ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • ensure that all data held on pupils on the is adequately protected • ensure that all data held on pupils on the school office machines have appropriate access controls in place

Teachers	□ embed e-Safety issues in all aspects of the curriculum and other school activities □ supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities) □ ensure that pupils are fully aware of research skills and are fully

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

1. Following the School's Behaviour Policy.
2. Discussion with the Head teacher.
3. Informing parents or carers.
4. Removal of Internet or computer access for a period.
5. Referral to Police.

- Any complaint about pupil misuse should be initially be reported to the class teacher.
- Any complaint about staff misuse is referred to the Head teacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school's child protection procedures.

Review and Monitoring

The e-Safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The Computing coordinator and Head teacher will be responsible for document ownership, review and updates.
- The e-Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-Safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum Pupil e-Safety curriculum

Snape Wood Primary and Nursery

- has a clear, progressive e-Safety education programme that covers a range of skills and behaviours appropriate to pupil age and experience, including:
- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- Understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files, such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- Understand why and how some people will 'groom'
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- To know how to report any abuse including peer-on-peer abuse and cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through reminders about the Acceptable Use Policy.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Ensure pupils only use school-approved systems and publish within appropriately secure / ageappropriate environments.

Staff and governor training

Snape Wood Primary School -

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-Safety issues and the school's e-Safety education program including annual updates and training throughout the year as practice develops and changes.
- Provides as part of the induction process, all new staff with information and guidance on the eSafeguarding and the school's Acceptable Use Policies.
- All computer users are to lock their devices if they step away from the screen e.g. to collect printing/ attend to other duties using CTRL + L.
- Staff are not to share user accounts and passwords under any circumstances in order to prevent sensitive data breaches.

Parent awareness and training

Snape Wood Primary School runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements in the autumn term
- Photograph and media sharing consent forms in the autumn term
- For any school performances, a verbal disclaimer must be given to ensure that the identities of e.g. looked-after children/witness protection are kept safe. (This might be as follows: "We know that you may wish to film your child in the performance, as these are precious moments, however, we request that you do not share your media on social networking sites, for example, as we have to safeguard the identity of some of our children).
- Information and guidance; in school newsletters; on the school web site
- Demonstrations, practical sessions held at school
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents

3. Expected Conduct and Incident management Expected conduct

At Snape Wood Primary School, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school
- Know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking /use of images and on cyber-bullying.

Staff, volunteers and contractors

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

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the eSafety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

At Snape Wood Primary School:

- There is strict monitoring and application of the e-Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes
- Support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-Safety issues
- Monitoring and reporting of e-Safety incidents takes place and contribute to developments in policy and practice in e-Safety within the school. When necessary the records are reviewed and reported to the school's senior leaders
- Parents/carers are specifically informed of e-Safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities - Police, Internet Watch Foundation and inform the LA. **4. Managing IT and Communication System**

Internet access, security (virus protection) and filtering Snape Wood Primary School:

- Has the educational filtered secure broadband connectivity through Capita Bytes and so connects to the 'private' National Education Network
- Uses a sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. Who has the rights to change to the filtering policy is logged and only available to staff with the approved 'web filtering management' status
- Uses the East Midlands Public Service Network to enable appropriate filtering for the age of the pupils

- Ensures network healthy through use of Microsoft anti-virus software and network set-up so staff and pupils cannot download executable files
- Uses DfE or LA approved systems such as S2S, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes
- Has blocked pupil access to music download or shopping sites - except those approved for educational purposes at a regional or national level, such as Audio Network
- Uses security time-outs on Internet access where useful
- Works in partnership with the Nottingham Local Authority to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses commonsense strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment
- Requires staff to preview websites before use [where not previously viewed or cached]. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the teacher. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or Nottingham City Helpdesk as necessary
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse - through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police, and the LA.

Network management (user access, backup)

Snape Wood Primary School

- Uses individual, audited log-ins for all users
- Has additional local network auditing software installed
- Ensures the Systems Administrator is up-to-date with LA services and policies
- Storage of all data within the school will conform to the UK data protection requirements
- Has daily back-up of school data (admin and curriculum)
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.
- Storage of all data complies with GPDR regulations as of 25/5/2018.

To ensure the network is used safely, Snape Wood Primary and Nursery School:

- Ensures staff read and sign that they have understood the school's e-Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password
- All children and staff have unique username and password
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download or shopping sites - except those approved for educational purposes
- Scans all equipment with anti-virus/spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the antivirus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any 'significant personal use' as defined by HM Revenue & Customs
- Maintains equipment to ensure Health and Safety is followed e.g. equipment installed and checked by approved Suppliers/LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEND coordinator - SEN data
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Has an automated system for the daily back up of MIS and finance systems and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
- Uses our broadband network for our CCTV system and have had set-up by approved partners
- Uses the DfE secure s2s website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network

- Our wireless network has been secured to industry standard Enterprise security level standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school IT systems regularly with regard to health and safety and security.

Passwords policy

- Snape Wood Primary School makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

Snape Wood Primary and Nursery School

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.sch.uk / head@schoolname.sch.uk /or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'etiquette' of using e-mail both in school and at home i.e. they are taught:

○ Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer

○ That an e-mail is a form of publishing where the message should be clear, short and concise

○ That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper

○ They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc

○ To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe

○ That they should think carefully before sending any attachments;

○ Embedding adverts is not allowed

○ That they must immediately tell a teacher responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature

○ Not to respond to malicious or threatening messages

- ○ Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
- ○ Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- ○ That forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LA e-mail systems on the school system
- Staff only use LA e-mail systems for professional purposes
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- We use secure, approved systems to transfer staff or pupil personal data
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used
- The sending of chain letters is not permitted ○ Embedding adverts is not allowed.
- All staff sign our School Agreement Form AUP to say they have read and understood the e-Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- ○ The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- ○ The school website complies with the statutory DfE guidelines for publications
- ○ Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- ○ The point of contact on the website is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published
- ○ Photographs published on the web do not have full names attached
- ○ We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Learning platform

- ○ Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- ○ Photographs and videos uploaded to the schools systems will only be accessible by members of the school community
- ○ In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

Social networking

- ○ Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to reduce the risk of loss of personal information.
- Staff should not make contact with parents via social media websites and apps. Any incidences of parents who make contact with staff should be reported directly to the headteacher.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices At Snape Wood Primary School:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in our Single Central Record
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed. This makes clear staffs responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/ Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. Where necessary we have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer.
- We use a 2-factor authentication for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.

- We use the LA approved company for disposal of equipment where any protected or restricted data has been held.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded. We are using secure file deletion software.

6. Equipment and Digital Content Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupil, parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Students use of personal devices

- The School strongly advises that pupil mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have mobile phone for their own safety. The device must be handed straight into the office when the pupil arrives at school and collected at the end of the day. Staff will not be held responsible to lost or stolen devices.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personallyowned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Any permitted images or files taken in school on staff handheld devices, including mobile phones and personal cameras must be downloaded from the device and deleted in school before the end of the day.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when supervised.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

At Snape Wood Primary and Nursery School:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

- Parents are not permitted to take photographs or to make a video recording for anything other than their own personal use e.g. with a view to selling videos of a school event eg at a school concert.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- We will periodically invite an official photographer into school to take portraits/photographs of individual children and/or class groups. The school will undertake its own risk assessment in terms of the validity of the photographer/agency involved and establish what checks/vetting has been undertaken e.g. DBS
- Staff sign the schools Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- As part of their work pupils will have access to the use of digital cameras. Any pictures that they take will be kept at school and the children will be taught about the need to keep these images private. When on school visits pupils are not allowed to take their own cameras or use cameras on phones. **Asset disposal**

Details of all school-owned hardware will be recorded in a hardware inventory.

All redundant equipment will be disposed of through an authorised agency. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

6. Digital Wellbeing Definition of Digital Wellbeing

Childnet.com defines digital wellbeing as follows:

Our overall wellbeing is determined by the physical and emotional experiences we have on a daily basis. As technology continues to be such a huge part of our lives, from the way we represent who we are to the interactions we have with others, it too has an impact on our wellbeing. This is often referred to as your 'digital wellbeing' or 'online wellness.'

It is essentially about having an awareness of how being online can make us feel and looking after ourselves and others when online. This can include recognising the impact being online can have on our emotions, mental wellbeing and even on our physical health and knowing what to do if something goes wrong. Our digital wellbeing can be influenced by the choices we make online, the content we see, the interactions we have with others and even how long we spend engaging with technology and the internet. ***Reports*** *have found that those who spend extended amounts of time online are more likely to see upsetting content, receive abusive comments or send abuse to others.*

Technology and the internet should be there to enhance and simplify our lives rather than be a cause of distraction, worry or upset. However, not all online experiences are positive for young people and this can have a negative impact on how they feel about themselves, their friendships and relationships and even how they see the wider world.

At Snape Wood Primary, we understand that extended lengths of time spent on digital devices can have a detrimental impact on the wellbeing of the child. As a school, we have a duty of care to ensure that every child is given equal opportunities to learning, and have a duty to report to the designated safeguarding lead if we feel that there is a safeguarding issue regarding the use of technology. This complements our Safeguarding policy and other policies mentioned previously.

Acceptable hours of communication for Staff

As explained above, technology should be an enhancement, not a tool for destruction and negativity. Email communication is a key form of communication at Snape Wood, however, the following protocol should be adhered to, in order to promote a health work-life balance:

- All staff must log into their emails when they first come into work in the morning, and check them at a suitable time throughout the day (i.e. lunchtimes and after 15:15) to keep apprised of communication in the school.
- Communication via email should not happen after the hours of 19:00 and before 07:00 each working day (unless in cases of emergency, in which case it might be more suitable to contact staff more directly).
- Staff should refrain from contacting other members of staff via email with regards to work matters at the weekend, unless there is a prior agreement that this is acceptable for all parties involved.
- There is no expectation on staff that emails will be read or responded to between the hours of 19:00 and 07:00 on weekdays and at any time on weekends.

National advice on limiting screen time for children The NHS recommend that:

- Restrict screen time (including TV, smartphones, tablets and video games) to less than 2 hours a day.
- Sleep 9 to 11 hours a night
- Do at least 1 hour of moderate to vigorous physical activity a day.

-source: https://www.nhs.uk/news/pregnancy-and-child/more-sleep-and-limiting-screen-time-mayimprove-childrensmental-abilities/ Last accessed: 3/2/20 15:03

Staff have a duty of care to report any concerns with regards to over-reliance on technology to a designated safeguarding lead.

Digital Wellbeing Group Roles and Responsibilities

The Digital Wellbeing group will assist the Digital Wellbeing Coordinator with:

- Developing and maintaining e-safety provision within the school Regular monitoring of e-safety incident logs.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an esafety incident taking place.
- Maintaining reports of e-safety incidents and creating a log of incidents to inform future e-safety developments.

The key responsibilities of a Digital Wellbeing coordinator include:

- Developing an e-safe culture
- Being the main point of contact on issues relating to e-safety
- Putting together and leading an e-safety team
- Raising awareness and understanding of e-safety issues amongst all stakeholders, including parents and carers.
- Embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities.
- Keeping up with relevant e-safety legislation
- Liaising with the local authority and other agencies as appropriate
- Reviewing and updating e-safety policies and procedures regularly